aws

Benutzerhandbuch

Amazon Lightsail

Amazon Lightsail: Benutzerhandbuch

Table of Contents

Was ist Amazon Lightsail?

Amazon Lightsail ist der einfachste Einstieg in Amazon Web Services (AWS) für alle, die Websites oder Webanwendungen erstellen müssen. Es enthält alles, was Sie für einen schnellen Start Ihres Projekts benötigen — Instanzen (virtuelle private Server), Containerdienste, verwaltete Datenbanken, Content Delivery Network (CDN) -Distributionen, Load Balancer, SSD-basierter Blockspeicher, statische IP-Adressen, DNS-Verwaltung registrierter Domains und Ressourcen-Snapshots (Backups) — zu einem niedrigen, vorhersehbaren monatlichen Preis.

Lightsail bietet auch Amazon Lightsail for Research an. Mit Lightsail for Research können Wissenschaftler und Forscher leistungsstarke virtuelle Computer in der erstellen. AWS Cloud Diese virtuellen Computer verfügen über vorinstallierte Forschungsanwendungen wie RStudio und Scilab. Weitere Informationen finden Sie im Amazon Lightsail for Research-Benutzerhandbuch.

Themen

Eigenschaften von Lightsail

Lightsail bietet die folgenden Funktionen auf hohem Niveau:

Instances

Lightsail bietet virtuelle private Server (Instanzen), die einfach einzurichten sind und durch die Leistung und Zuverlässigkeit von unterstützt werden. AWS Sie können Ihre Website, Webanwendung oder Ihr Projekt in wenigen Minuten starten und Ihre Instanz über die intuitive Lightsail-Konsole oder API verwalten.

Bei der Erstellung Ihrer Instanz verwenden Sie click-to-launch ein einfaches Betriebssystem (OS), eine vorkonfigurierte Anwendung oder einen Entwicklungsstapel, z. B. Windows, Plesk, LAMP

WordPress, Nginx und mehr. Jede Lightsail-Instanz verfügt über eine integrierte Firewall, mit der Sie den Datenverkehr zu Ihren Instances auf der Grundlage von Quell-IP, Port und Protokoll zulassen oder einschränken können. Weitere Informationen

Container

Führen Sie containerisierte Anwendungen in der Cloud aus und greifen Sie sicher darauf zu. Ein Container ist eine Standardeinheit von Software, die Code und seine Abhängigkeiten zusammen packt, sodass die Anwendung schnell und zuverlässig von einer Computerumgebung zur anderen ausgeführt wird. Weitere Informationen

Load Balancers

Leiten Sie den Web-Traffic zwischen Ihren Instanzen, sodass Ihre Websites und Anwendungen Schwankungen des Datenverkehrs aufnehmen können, vor Ausfällen geschützt sind und ein nahtloses Besuchererlebnis bieten. Weitere Informationen

Verwaltete Datenbanken

Lightsail bietet einen vollständig konfigurierten Plan für MySQL- oder PostgreSQL-Datenbanken, der Speicher-, Verarbeitungs-, Speicher- und Übertragungszuschüsse umfasst. Mit Lightsail-verwalteten Datenbanken können Sie Ihre Datenbanken problemlos unabhängig von Ihren virtuellen Servern skalieren, die Anwendungsverfügbarkeit verbessern oder eigenständige Datenbanken in der Cloud ausführen. Weitere Informationen

Block- und Objektspeicher

Lightsail bietet sowohl Block- als auch Objektspeicher. Mit hochverfügbarem SSD-gestütztem Speicher für Ihren virtuellen Linux- oder Windows-Server können Sie Ihren Speicher schnell und einfach skalieren. Weitere Informationen

Mit Lightsail Object Storage Buckets können Sie Objekte jederzeit und von überall im Internet speichern und abrufen. Sie können auch statische Inhalte in der Cloud hosten. Weitere Informationen

CDN-Distributionen

Lightsail ermöglicht Content Delivery Network (CDN) -Distributionen, die auf derselben Infrastruktur wie Amazon basieren. CloudFront Sie können Ihre Inhalte ganz einfach an ein globales Publikum verteilen, indem Sie Proxyserver auf der ganzen Welt einrichten, sodass Ihre Benutzer geografisch näher an ihnen auf Ihre Website zugreifen können, wodurch die Latenz reduziert wird. Weitere Informationen

Zugriff auf AWS-Services

> Lightsail verwendet spezielle Funktionen wie Instanzen, verwaltete Datenbanken und Load Balancer, um den Einstieg zu erleichtern. Das heißt aber nicht, dass Sie auf diese Optionen beschränkt sind — Sie können Ihr Lightsail-Projekt über Amazon VPC-Peering mit einigen der AWS über 90 anderen Services integrieren. Weitere Informationen

Weitere Informationen zu Lightsail finden Sie unter Amazon Lightsail.

Für wen ist Lightsail gedacht?

Lightsail ist für alle da. Sie können ein Image für Ihre Lightsail-Instanz auswählen, das Ihr Projekt beschleunigt, sodass Sie nicht so viel Zeit mit der Installation von Software oder Frameworks verbringen müssen.

Wenn Sie als Einzelentwickler oder Bastler an einem persönlichen Projekt arbeiten, kann Lightsail Sie bei der Bereitstellung und Verwaltung grundlegender Cloud-Ressourcen unterstützen. Möglicherweise wollen Sie auch Cloud-Services kennenlernen oder damit experimentieren, wie z. B. virtuellen Maschinen, Domains oder Netzwerken. Lightsail bietet einen schnellen Einstieg.

Lightsail bietet Images mit Basisbetriebssystemen, Entwicklungs-Stacks wie LAMP, LEMP (Nginx) und SQL Server Express sowie Anwendungen wie WordPress Drupal und Magento. Ausführlichere Informationen zu der auf den einzelnen Images installierten Software finden Sie unter Wählen Sie ein Lightsail-Instanz-Image aus.

Wenn Ihr Projekt wächst, können Sie Blockspeicherfestplatten hinzufügen und sie an Ihre Lightsail-Instanz anhängen. Sie können Snapshots von diesen Instances und Datenträgern erstellen und anhand dieser Snapshots auf einfache Weise neue Instances erstellen. Sie können Ihre VPC auch per Peering verbinden, sodass Ihre Lightsail-Instances andere AWS Ressourcen außerhalb von Lightsail nutzen können.

Sie können auch einen Lightsail-Load Balancer erstellen und Zielinstanzen anhängen, um eine hochverfügbare Anwendung zu erstellen. Außerdem können Sie die Load Balancer konfigurieren, um verschlüsselten HTTPS-Datenverkehr, Sitzungspersistenz, Zustandsprüfungen und mehr zu verarbeiten.

Lightsail öffnen

Sie können Ihre Lightsail-Ressourcen mit den folgenden Schnittstellen erstellen und verwalten:

Amazon Lightsail-Konsole

Eine einfache Weboberfläche zum Erstellen und Verwalten von Lightsail-Instanzen und -Ressourcen. Wenn Sie sich für ein AWS Konto angemeldet haben, können Sie auf die Lightsail-Konsole zugreifen, indem Sie sich bei der anmelden AWS Management Console und auf der Konsolen-Startseite Lightsail auswählen.

AWS Command Line Interface

Ermöglicht Ihnen die Interaktion mit AWS Diensten mithilfe von Befehlen in Ihrer Befehlszeilen-Shell. Es wird auf Windows, Mac und Linux unterstützt. Weitere Informationen zur AWS CLI finden Sie im Benutzerhandbuch zu AWS Command Line Interface. Sie finden die Lightsail-Befehle in der Amazon Lightsail-API-Referenz.

AWS Tools for PowerShell

Eine Reihe von PowerShell Modulen, die auf den Funktionen basieren, die von der bereitgestellt werden. AWS SDK for .NET Mit den Tools für PowerShell können Sie über die PowerShell Befehlszeile Skripts für Operationen auf Ihren AWS Ressourcen erstellen. Informationen zu den ersten Schritten finden Sie im AWS Tools for Windows PowerShell -Benutzerhandbuch. Sie finden die Cmdlets für Lightsail in der Cmdlet-Referenz.AWS Tools for PowerShell

Abfrage-API

Lightsail bietet eine Abfrage-API. Diese Abfragen sind HTTP- oder HTTPS-Anfragen, die die HTTP-Verben GET oder POST und einen Abfrageparameter namens `Action` verwenden. Weitere Informationen zu den API-Aktionen für Lightsail finden Sie unter Aktionen in der Amazon Lightsail-API-Referenz.

AWS SDKs

Wenn Sie es vorziehen, Anwendungen mithilfe sprachspezifischer APIs zu erstellen, anstatt eine Anfrage über HTTP oder HTTPS zu stellen, AWS bietet diese Website Bibliotheken, Beispielcode, Tutorials und andere Ressourcen für Softwareentwickler. Diese Bibliotheken bieten grundlegende Funktionen zur Automatisierung von Aufgaben, z. B. kryptografisches Signieren von Anfragen, Wiederholen von Anfragen und Behandlung von Fehlermeldungen. Dadurch wird Ihnen der Einstieg erleichtert. Weitere Informationen finden Sie unter Tools, auf denen Sie aufbauen können. AWS

Erste Schritte mit Lightsail

Nachdem Sie Lightsail eingerichtet haben, können Sie die einzelnen Schritte ausführen, um eine Tutorial: Erste Schritte mit Amazon Lightsail-Instances Instance zu starten, eine Verbindung herzustellen und sie zu bereinigen.

Zugehörige Services

Sie können Lightsail-Ressourcen wie Instanzen und Festplatten direkt mit Lightsail bereitstellen. Darüber hinaus können Sie Ressourcen mithilfe anderer AWS Dienste bereitstellen, z. B. mit den folgenden:

- Amazon EC2

  Stellt Rechenkapazität — im wahrsten Sinne des Wortes Server in den Rechenzentren von Amazon — zur Verfügung, die Sie zum Aufbau und Hosten Ihrer Softwaresysteme verwenden. Einen Vergleich von Lightsail und Amazon EC2 finden Sie unter Amazon Lightsail oder Amazon EC2.

- Amazon EC2 Auto Scaling

  Hilft Ihnen sicherzustellen, dass Sie die richtige Anzahl von Amazon-EC2-Instances zur Verfügung haben, um die Auslastung Ihrer Anwendung zu bewältigen.

- Elastic Load Balancing

  Verteilen Sie eingehenden Anwendungsdatenverkehr automatisch auf mehrere Instances.

- Amazon Relational Database Service (Amazon RDS)

  Führen Sie die Einrichtung, den Betrieb und die Skalierung einer verwalteten relationalen Datenbank in der Cloud durch.

- Amazon Elastic Container Service (Amazon ECS)

  Stellen Sie containerisierte Anwendungen auf einem Cluster von Amazon EC2 EC2-Instances bereit, verwalten und skalieren Sie sie.

Kostenvoranschläge, Abrechnung und Kostenoptimierung

Um Schätzungen für Ihre Anwendungsfälle zu erstellen, AWS verwenden Sie den. AWS Pricing Calculator

Um Ihre Rechnung anzuzeigen, navigieren Sie zu Fakturierungs- und Kostenverwaltungs-Dashboard in der AWS Billing and Cost Management -Konsole. Ihre Abrechnung enthält Links zu Nutzungsberichten mit Details zu Ihrer Abrechnung. Weitere Informationen zur AWS Kontoabrechnung finden Sie im AWS Billing and Cost Management-Benutzerhandbuch.

Wenn Sie Fragen zu AWS Abrechnung, Konten und Veranstaltungen haben, wenden Sie sich an den AWS Support.

Mithilfe von können Sie die Kosten, Sicherheit und Leistung Ihrer AWS Umgebung optimieren AWS Trusted Advisor.

Einrichten Ihres AWS-Kontos zur Verwendung von Amazon Lightsail

Wenn Sie ein neuer AWS-Kunde sind, müssen Sie die Einrichtungsvoraussetzungen erfüllen, bevor Sie mit der Nutzung von Amazon Lightsail beginnen. Für diese Einrichtungsverfahren verwenden Sie den AWS Identity and Access Management (IAM)-Service. Umfassende Informationen zu IAM finden Sie im IAM-Benutzerhandbuch.

Themen

Registrieren bei AWS

Wenn Sie kein AWS-Konto haben, führen Sie die folgenden Schritte zum Erstellen durch.

Anmeldung für ein AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für ein AWS-Konto anmelden, wird ein Root-Benutzer des AWS-Kontos erstellt. Der Stammbenutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Methode zur Gewährleistung der Sicherheit sollten Sie den administrativen Zugriff einem administrativen Benutzer zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, die einen Root-Benutzerzugriff erfordern.

Erstellen eines IAM-Benutzers

Wählen Sie zum Erstellen eines Administratorbenutzers eine der folgenden Optionen aus.

Wählen Sie eine Möglichkeit zur Verwaltung Ihres Administrators aus.	Bis	Von	Sie können auch
Im IAM Identity Center (Empfohlen)	Verwendung von kurzfristigen Anmeldeinformationen für den Zugriff auf AWS. Dies steht im Einklang mit den bewährten Methoden für die Sicherheit. Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.	Beachtung der Anweisungen unter Erste Schritte im AWS IAM Identity Center-Benutzerhandbuch.	Programmgesteuerten Zugriff unter Berücksichtigung der Informationen im Abschnitt Konfigurieren von AWS CLI für die Verwendung vonAWS IAM Identity Center im AWS Command Line Interface-Benutzerhandbuch konfigurieren.
In IAM (Nicht empfohlen)	Verwendung von langfristigen Anmeldeinformationen für den Zugriff auf AWS.	Beachtung der Anweisungen unter Erstellen Ihres ersten IAM-Administratorbenutzers und Ihrer ersten Benutzergruppe im IAM-Benutzerhandbuch.	Programmgesteuerten Zugriff unter Verwendung der Informationen unter Verwalten der Zugriffsschlüssel für IAM-Benutzer im IAM-Benutzerhandbuch konfigurieren.

Tutorial: Erste Schritte mit Amazon Lightsail-Instances

In diesem Tutorial erfahren Sie, wie Sie eine Amazon Lightsail-Instance erstellen, eine Verbindung zu ihr herstellen und sie verwenden. In Lightsail ist eine Instance ein virtueller privater Server (auch als virtuelle Maschine bezeichnet). Sie erstellen und verwalten Lightsail-Instances in der AWS Cloud. Wenn Sie Ihre Instance erstellen, wählen Sie ein Image aus, das ein Betriebssystem (OS) hat. Sie können auch ein Instance-Image wählen, das eine Anwendung oder einen Entwicklungs-Stack enthält, einschließlich des Basis-Betriebssystems.

Für die Instance, die Sie in diesem Tutorial erstellen, fallen ab dem Zeitpunkt, an dem Sie sie erstellen, bis zu dem Zeitpunkt, an dem Sie sie löschen, Nutzungsgebühren an. Das Löschen ist der letzte Schritt in diesem Tutorial. Weitere Informationen zu Preisen finden Sie unter Lightsail-Preise.

Themen

Schritt 1: Erfüllen der Voraussetzungen

Wenn Sie ein -AWSNeukunde sind, müssen Sie die Einrichtungsvoraussetzungen erfüllen, bevor Sie mit der Verwendung von Amazon Lightsail beginnen. Weitere Informationen finden Sie unter Einrichten Ihres AWS-Kontos zur Verwendung von Amazon Lightsail.

Schritt 2: Erstellen einer Instance

Sie können eine Instance mithilfe der Lightsail-Konsole erstellen, wie im folgenden Verfahren beschrieben. Diese Anleitung soll Ihnen helfen, Ihre erste Instance schnell zu starten. Wir empfehlen

außerdem, sich mit den verfügbaren Anwendungen und Hardwareplänen vertraut zu machen. Weitere Informationen finden Sie unter Wählen Sie ein Amazon Lightsail-Instance-Image.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Website Create instance (Instance erstellen).
3. Wählen Sie einen Standort für Ihre Instance (eine AWS-Region und eine Availability Zone). Wählen Sie eine AWS-Region, die sich in der Nähe Ihres physischen Standorts befindet, um die Latenz zu reduzieren.

   Wählen Sie Verändern von AWS-Region und Availability Zone aus, um den Speicherort für die Instance zu ändern.
4. Wählen Sie eine Anwendung (Apps + OS) oder ein Betriebssystem (Nur OS) aus.

   Weitere Informationen zu Lightsail-Instance-Images finden Sie unter Wählen Sie ein Amazon Lightsail-Instance-Image.
5. Wählen Sie Ihren Instance-Plan aus.

   Wählen Sie aus, ob Ihre Instance Dual-Stack-Netzwerke (IPv4 und IPv6) oder IPv6-onlyNetzwerke verwendet. Einige Lightsail-Vorlagen unterstützen derzeit kein IPv6-onlyNetzwerk. Informationen dazu, welche Vorlagen IPv6-onlyNetzwerke unterstützen, finden Sie unter Wählen Sie ein Amazon Lightsail-Instance-Image.

   Sie können den Lightsail-Plan 3,50 USD einen Monat lang kostenlos (bis zu 750 Stunden) testen. Wir fügen Ihrem Konto einen kostenlosen Monat hinzu. Erfahren Sie mehr auf unserer Lightsail-Preisgestaltungsseite.
6. Geben Sie einen Namen für Ihre Instance ein.

   Ressourcennamen:

   - Muss in jedem AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.
7. Wählen Sie Create instance (Instance erstellen).

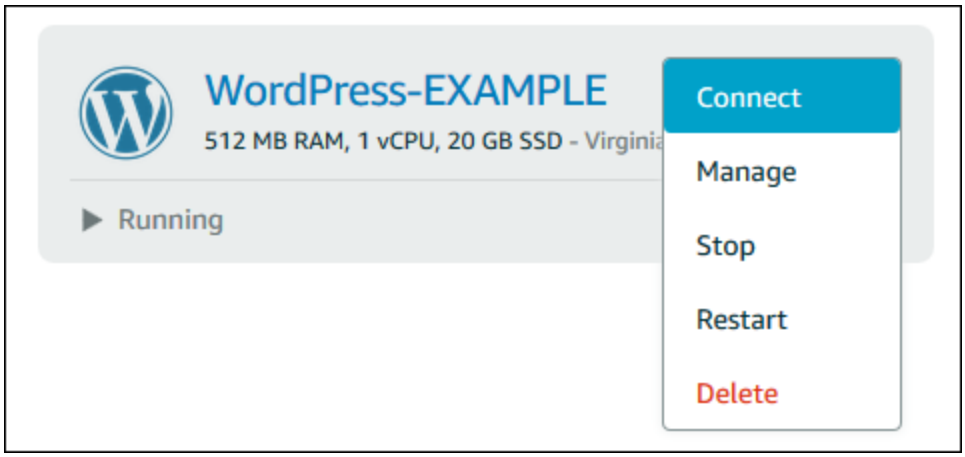
Innerhalb weniger Minuten ist Ihre Lightsail-Instance bereit und Sie können eine Verbindung zu ihr herstellen.

Schritt 3: Verbindung mit Ihrer Instance herstellen

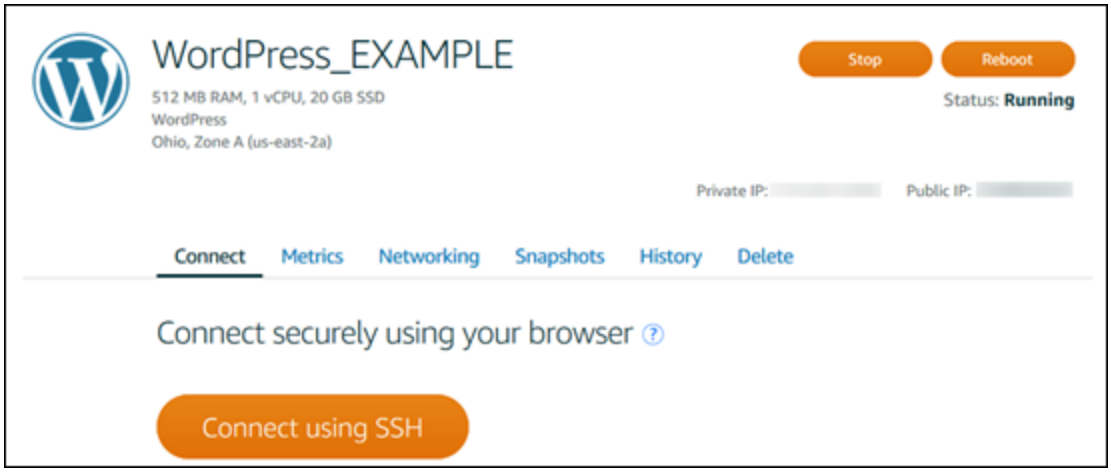
1.

> **Note**
>
> Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um über IPv6 SSH oder RDP in Ihre Instance zu senden. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

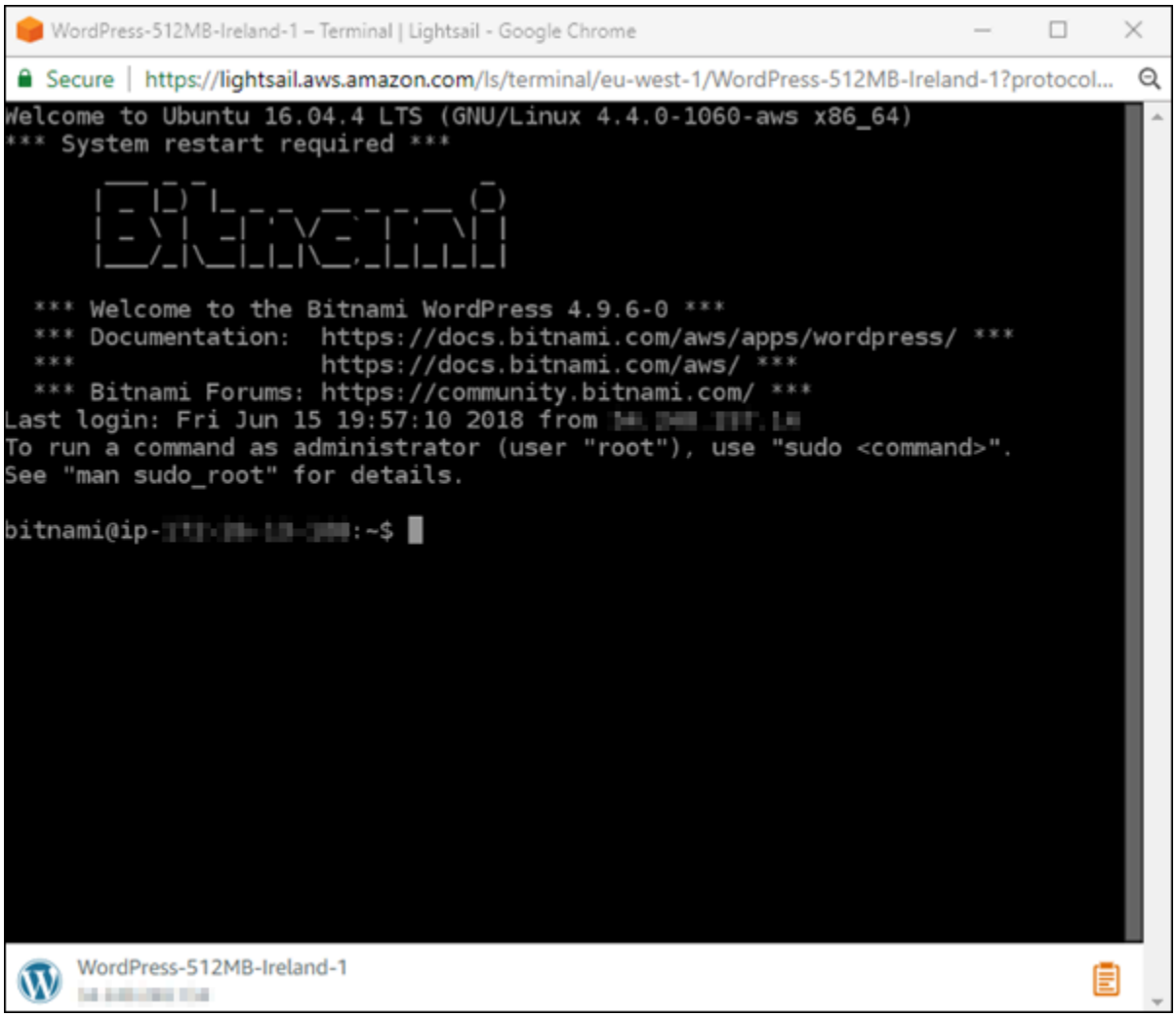
Wählen Sie auf der Lightsail-Startseite das Menü rechts neben dem Namen Ihrer Instance und dann Verbinden aus.



Alternativ können Sie die Verwaltungsseite für Ihre Instance öffnen und dort auf die Registerkarte Connect (Verbinden) gehen.



2. Sie können jetzt Befehle in das Terminal eingeben und Ihre Lightsail-Instance verwalten, ohne einen SSH-Client einzurichten.



Um zu erfahren, wie Sie eine Verbindung herstellen, um Ihrem virtuellen Computer zusätzlichen Speicherplatz hinzuzufügen, fahren Sie mit dem nächsten Schritt dieses Tutorials fort.

Schritt 4: Hinzufügen von Speicher zu Ihrer Instance

Lightsail bietet Volumes für die Speicherung auf Blockebene (Festplatten), die Sie an eine Instance anfügen können. Obwohl Ihre Instance mit einer Systemfestplatte geliefert wird, können Sie zusätzliche Speicherfestplatten hinzufügen, wenn sich Ihre Anforderungen ändern. Sie können eine Festplatte auch von einer Instance trennen und einer anderen Instance zuordnen.

Nachdem Sie einen zusätzlichen Datenträger erstellt haben, müssen Sie eine Verbindung zu Ihrer Lightsail-Instance herstellen, um den Datenträger zu formatieren und zu mounten.

Weitere Informationen zum Erstellen, Anhängen und Verwalten einer Festplatte finden Sie unter Erstellen von zusätzlichen Blockspeicherdatenträgern und Anfügen an Ihre Linux-basierte Lightsail-Instance.

Fahren Sie mit dem nächsten Schritt dieses Tutorials fort, um mehr über die Sicherung Ihres virtuellen Computers zu erfahren.

Schritt 5: Erstellen Sie einen Snapshot

Snapshots sind eine point-in-time Kopie Ihrer Daten. Sie können Snapshots Ihrer Instances erstellen und diese als Baselines für die Erstellung neuer Instances oder für Datensicherungen verwenden. Ein Snapshot enthält alle Daten, die erforderlich sind, um Ihre Instance wiederherzustellen (von dem Zeitpunkt, an dem der Snapshot erstellt wurde).

Weitere Informationen zum Erstellen und Verwalten von Snapshots finden Sie unter Erstellen eines Snapshots Ihrer Linux-/Unix-basierten Lightsail-Instance.

Um zu erfahren, wie Sie Ihre virtuellen Computer-Ressourcen bereinigen, fahren Sie mit dem nächsten Schritt dieses Tutorials fort.

Schritt 6: Bereinigen

Nachdem Sie alle Schritte für die Instance abgeschlossen haben, die Sie für dieses Tutorial erstellt haben, können Sie sie löschen. Dadurch fallen keine Gebühren für die Instance an, wenn Sie sie nicht benötigen.

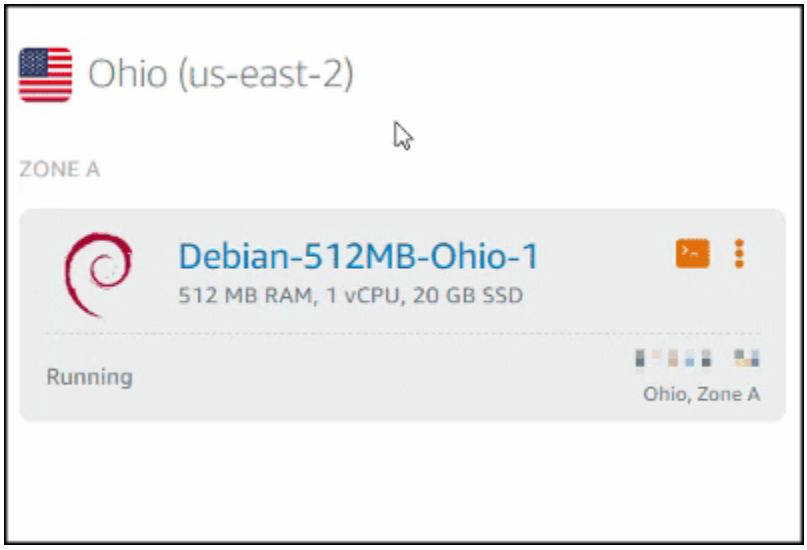
Durch das Löschen einer Instance werden die zugehörigen Snapshots oder angeschlossenen Festplatten nicht gelöscht. Wenn Sie für dieses Tutorial Snapshots und Festplatten erstellt haben, sollten Sie diese ebenfalls löschen.

Um Ihre Instance zur späteren Verwendung zu speichern, aber um Gebühren zu vermeiden, können Sie die Instance anhalten, anstatt sie zu löschen. Dann können Sie sie später erneut starten. Weitere Informationen zu Preisen finden Sie unter Lightsail-Preise.

> **Important**
>
> Das Löschen einer Lightsail-Ressource ist eine permanente Aktion. Die gelöschten Daten können nicht wiederhergestellt werden. Wenn Sie die Daten später benötigen, erstellen Sie

einen Snapshot Ihres virtuellen Computers, bevor Sie ihn löschen. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Linux-/Unix-basierten Lightsail-Instance.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie für die zu löschende Instance das Aktionsmenü-Symbol (⋮) und dann Delete (Löschen).



4. Wählen Sie Yes, delete (Ja, löschen) zum Bestätigen der Löschung aus.

Nächste Schritte

Verwenden Sie die folgenden Themen, um mit Amazon Lightsail Linux- und Windows-basierten Instances zu beginnen.

- Erste Schritte mit Linux/Unix-basierten Instances in Amazon Lightsail
- Erste Schritte mit Windows Server-basierten Instances in Amazon Lightsail

Erste Schritte mit Linux/Unix-basierten Instances in Amazon Lightsail

Sie können innerhalb von Sekunden eine Linux/Unix-basierte Lightsail-Instance (einen Virtual Private Server) erstellen, auf der eine Anwendung wie WordPress oder ein Entwicklungs-Stack wie LAMP

ausgeführt wird. Nachdem Ihre Instance gestartet wurde, können Sie über SSH eine Verbindung zu ihr herstellen, ohne Lightsail zu verlassen. Das geht so:

Informationen zum Erstellen einer Windows-basierten Instance finden Sie unter Erste Schritte mit Windows-basierten Instances in Amazon Lightsail.

Erstellen einer Linux-basierten Instance

1. Wählen Sie auf der Website Create instance (Instance erstellen).
2. Wählen Sie einen Speicherort für Ihre Instance aus (eine AWS-Region und Availability Zone).

   Wählen Sie Ändern AWS-Region und Availability Zone, um Ihre Instance an einem anderen Ort zu erstellen.
3. Optional können Sie die Availability Zone wechseln.

   Wählen Sie „Availability Zone ändern“.
4. Wählen Sie die Linux-Plattform aus.
5. Wählen Sie eine Anwendung (Apps + OS) oder ein Betriebssystem (OS Only (Nur OS)) aus.

   Weitere Informationen zu Lightsail-Instance-Images finden Sie unter Auswählen eines Amazon Lightsail-Instance-Images.
6. Wählen Sie Ihren Instance-Plan aus.

   Wählen Sie aus, ob Ihre Instance Dual-Stack-Netzwerke (IPv4 und IPv6) oder IPv6-onlyNetzwerke verwendet. Einige Lightsail-Vorlagen unterstützen derzeit kein IPv6-onlyNetzwerk. Informationen dazu, welche Vorlagen IPv6-onlyNetzwerke unterstützen, finden Sie unter Wählen Sie ein Amazon Lightsail-Instance-Image.

   Sie können den Lightsail-Plan 3,50 USD einen Monat lang kostenlos (bis zu 750 Stunden) testen. Wir fügen Ihrem Konto einen kostenlosen Monat hinzu. Erfahren Sie mehr auf unserer Lightsail-Preisgestaltungsseite.

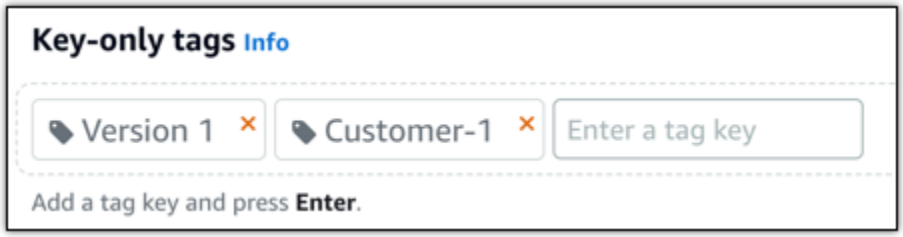
   > **Note**
   >
   > Im Rahmen des AWS kostenlosen Kontingents für können Sie kostenlos mit Amazon Lightsail für ausgewählte Instance-Pakete beginnen. Weitere Informationen finden Sie unter AWS Kostenloses Kontingent auf der Seite Amazon Lightsail – Preise.
7. Geben Sie einen Namen für Ihre Instance ein.

Ressourcennamen:

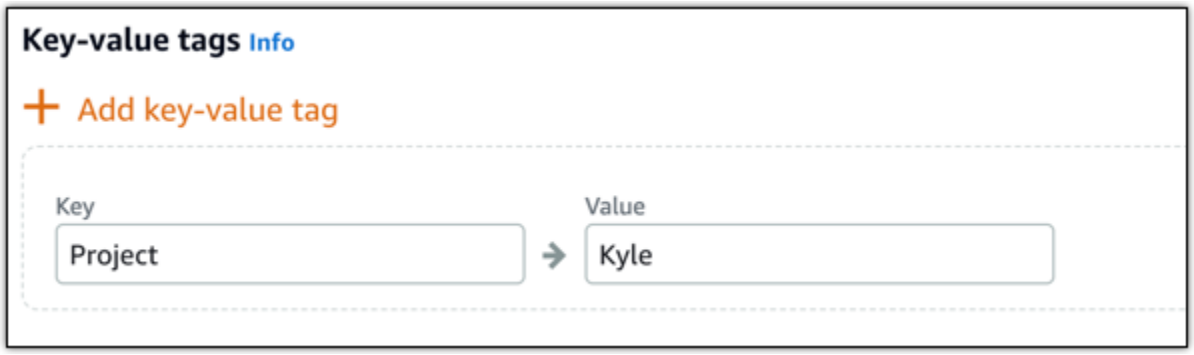
- Muss in jedem AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
- Muss zwischen 2 und 255 Zeichen enthalten.
- Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
- Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

8. Wählen Sie eine der folgenden Optionen, um Ihrer Instance Tags hinzuzufügen:

- Nur-Schlüssel-Tags hinzufügen. Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie X, um alle Tags zu entfernen, die Sie nicht behalten möchten.



- Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Schlüssel-Wert-Tags können nur einzeln hinzugefügt werden. Wählen Sie Schlüssel-Wert-Tag hinzufügen, um weitere Schlüssel-Wert-Tags hinzuzufügen, oder wählen Sie X, um alle Tags zu entfernen, die Sie nicht behalten möchten.



> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

9. Wählen Sie Create instance (Instance erstellen).

   Informationen zu erweiterten Erstellungsoptionen finden Sie unter Verwenden eines Startskripts zum Konfigurieren Ihrer Amazon Lightsail-Instance beim Start oder Einrichten von SSH für Ihre Linux/Unix-basierten Lightsail-Instances.

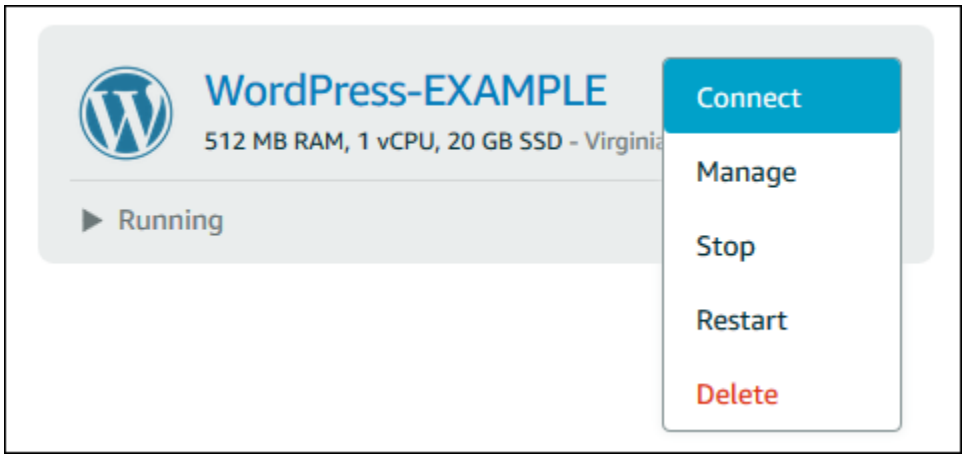
Innerhalb weniger Minuten ist Ihre Lightsail-Instance bereit und Sie können sich über SSH mit ihr verbinden, ohne Lightsail zu verlassen!

Herstellen einer Verbindung zu Ihrer Instance

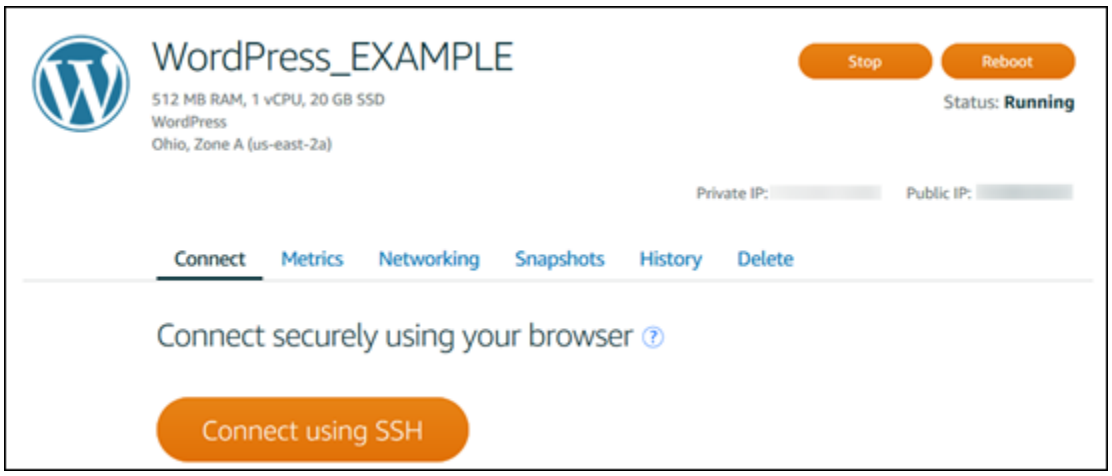
1.

> **Note**
>
> Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um SSH oder RDP über IPv6 in Ihre Instance zu übertragen. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

   Wählen Sie auf der Lightsail-Startseite das Menü rechts neben dem Namen Ihrer Instance und dann Verbinden aus.

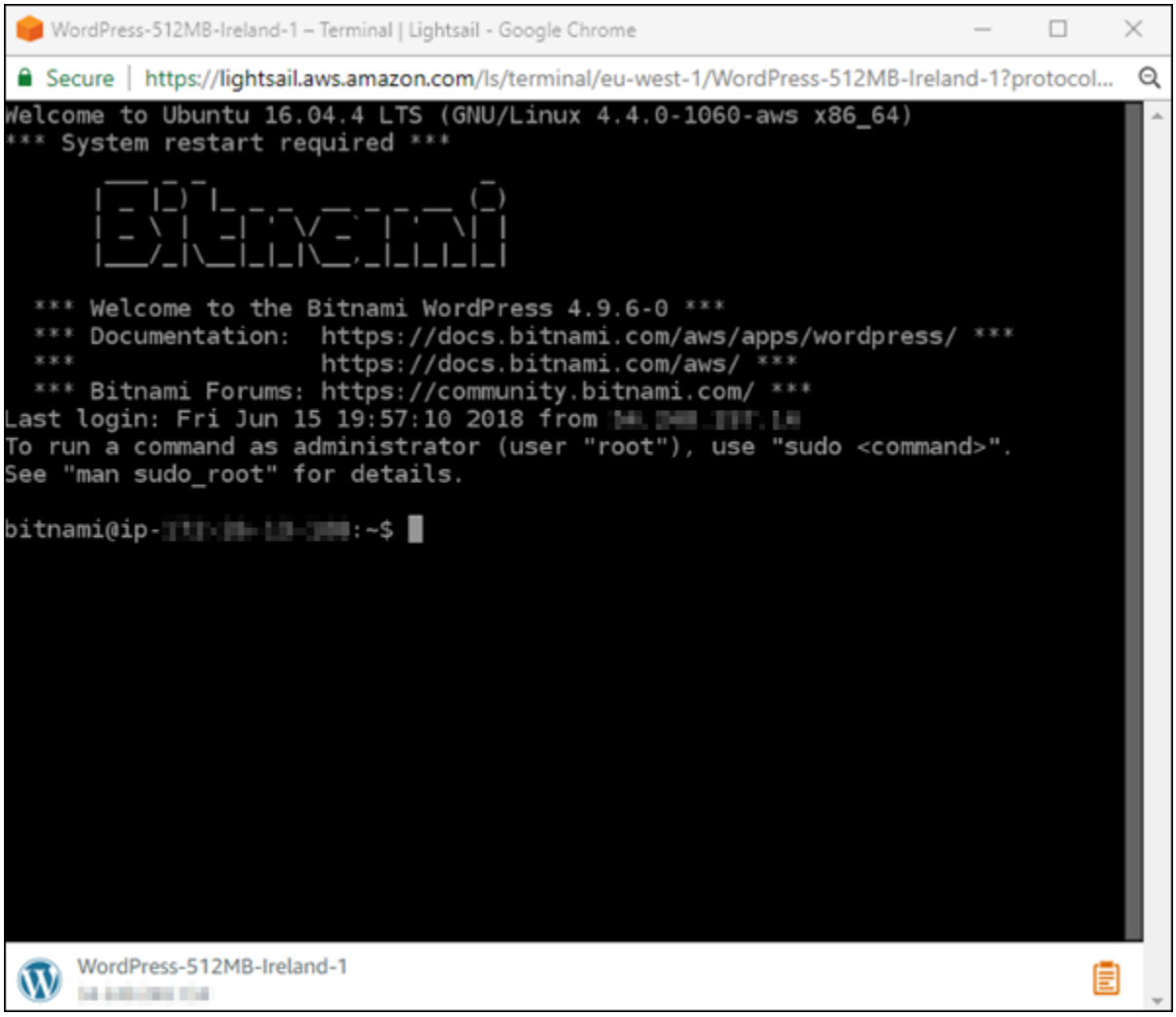


   Alternativ können Sie die Verwaltungsseite für Ihre Instance öffnen und dort auf die Registerkarte Connect (Verbinden) gehen.



> **Note**
>
> Um über einen SSH-Client wie PuTTY eine Verbindung zu Ihrer Instance herzustellen, können Sie die folgenden Schritte ausführen: PuTTY einrichten, um eine Verbindung zu Ihrer Lightsail-Instance herzustellen.

2. Jetzt können Sie Befehle in das Terminal eingeben und Ihre Lightsail-Instance verwalten, ohne einen SSH-Client einzurichten.



Nächste Schritte

Nachdem Sie eine Verbindung mit der Instance eingerichtet haben, sind Ihre nächsten Schritte davon abhängig, wie Sie sie verwenden möchten. Beispielsweise:

- the section called “WordPress” , wenn Sie einen Blog erstellen.
- Erstellen Sie eine statische IP-Adresse für Ihre Instance, damit sie bei jedem Neustart Ihrer Lightsail-Instance dieselbe IP-Adresse beibehält.
- Erstellen eines Snapshots Ihrer Instance als Sicherung.

Erste Schritte mit Windows Server-basierten Instances in Amazon Lightsail

Sie können Lightsail-Instances erstellen, auf denen das Windows Server-Betriebssystem (OS) ausgeführt wird. Es stehen zwei Betriebssystemvorlagen zur Auswahl: Windows Server 2022, Windows Server 2019 und Windows Server 2016. Zusätzlich stehen Vorlagen zur Verfügung, die mit SQL Server 2022, 2019 und 2016 Express vorkonfiguriert sind.

In diesem Thema finden Sie Informationen zum Auswählen der Software, Erstellen Ihrer Windows Server-basierten Instance und zum Herstellen einer Verbindung.

Weitere Informationen über Windows Server in AWS

Auswählen einer Windows Server-basierten Instance

Es gibt drei Optionen zum Erstellen einer Windows Server-basierten Instance in Lightsail.

Windows Server 2022

Lightsail unter Windows Server ist eine schnelle und zuverlässige Umgebung für die Bereitstellung von Anwendungen mit der Microsoft Web Platform. Mit Lightsail können Sie jede kompatible Windows-basierte Lösung auf der leistungsstarken, zuverlässigen und kosteneffektiven AWS Cloud Computing-Plattform ausführen. Häufige Windows-Anwendungsfälle umfassen Enterprise-Windows-basiertes Anwendungshosting, Website- und Webservice-Hosting, Datenverarbeitung, verteiltes Testen, ASP.NET-Anwendungshosting und jede andere Windows-Software, die Anwendungen erfordert.

Weitere Informationen über das Windows-Server-2022-Image

Windows Server 2019

Sofern Sie nicht aus irgendeinem Grund den Windows Server 2012 R2 oder Windows Server 2016 ausführen müssen, empfehlen wir die Verwendung der neuesten Version von Windows Server 2019.

Lightsail unter Windows Server ist eine schnelle und zuverlässige Umgebung für die Bereitstellung von Anwendungen mit der Microsoft Web Platform. Mit Lightsail können Sie jede kompatible Windows-basierte Lösung auf der leistungsstarken, zuverlässigen und kostengünstigen Cloud-Computing-Plattform von AWS ausführen. Häufige Windows-Anwendungsfälle umfassen Enterprise-Windows-basiertes Anwendungs-Hosting, Website- und Webservice-Hosting,

Datenverarbeitung, Transcodierung von Medien, verteiltes Testen, ASP.NET-Anwendungs-Hosting und jede andere Windows-Software, die Anwendungen erfordert.

Weitere Informationen über das Windows-Server-2019-Image

Windows Server 2016

Lightsail unter Windows Server ist eine schnelle und zuverlässige Umgebung für die Bereitstellung von Anwendungen mit der Microsoft Web Platform. Mit Lightsail können Sie jede kompatible Windows-basierte Lösung auf der leistungsstarken, zuverlässigen und kostengünstigen Cloud-Computing-Plattform von AWS ausführen. Häufige Windows-Anwendungsfälle umfassen Enterprise-Windows-basiertes Anwendungs-Hosting, Website- und Webservice-Hosting, Datenverarbeitung, Transcodierung von Medien, verteiltes Testen, ASP.NET-Anwendungs-Hosting und jede andere Windows-Software, die Anwendungen erfordert.

Weitere Informationen über das Windows Server 2016-Image

SQL Server Express 2022

SQL Server Express ist ein relationales Datenbankverwaltungssystem, das kostenlos heruntergeladen, verteilt und verwendet werden kann. Es besteht aus einer Datenbank, die speziell auf eingebettete und kleinere Anwendungen ausgerichtet ist. Dieses Lightsail-Image wird auf einem Basisbetriebssystem von Windows Server 2022 ausgeführt.

Weitere Informationen zum Image von SQL Server Express 2022

SQL Server Express 2019

SQL Server Express ist ein relationales Datenbankverwaltungssystem, das kostenlos heruntergeladen, verteilt und verwendet werden kann. Es besteht aus einer Datenbank, die speziell auf eingebettete und kleinere Anwendungen ausgerichtet ist. Dieses Lightsail-Image wird auf einem Basisbetriebssystem von Windows Server 2022 ausgeführt.

Weitere Informationen zum Image von SQL Server Express 2019

SQL Server Express 2016

SQL Server Express ist ein relationales Datenbankverwaltungssystem, das kostenlos heruntergeladen, verteilt und verwendet werden kann. Es besteht aus einer Datenbank, die speziell auf eingebettete und kleinere Anwendungen ausgerichtet ist. Dieses Lightsail-Image wird auf einem Basisbetriebssystem von Windows Server 2016 ausgeführt.

Weitere Informationen über das SQL Server Express-Image

Erstellen einer Windows Server-basierten -Instance

Sie können eine Windows Server-basierte Instance mit der Lightsail-Konsole oder mit der AWS Command Line Interface (AWS CLI) erstellen.

So erstellen Sie eine Instance mit der Konsole

1. Melden Sie sich bei Lightsail an und wechseln Sie dann zur -Startseite.
2. Wählen Sie Create instance (Instance erstellen).
3. Wählen Sie eine aus, AWS-Region in der Sie Ihre Windows Server-basierte Lightsail-Instance erstellen möchten.

   Beispiel: `Ohio (us-east-2)`
4. Wählen Sie die Microsoft Windows-Plattform aus.
5. Zum Festlegen der Vorlage für Windows Server 2022, Windows Server 2019, und Windows Server 2016 wählen Sie Nur OS aus.

   Zum Festlegen der SQL Server Express-Vorlage wählen Sie Apps + OS aus.
6. Wählen Sie Ihren Instance-Plan aus.

   Wählen Sie aus, ob Ihre Instance Dual-Stack-Netzwerke (IPv4 und IPv6) oder IPv6-onlyNetzwerke verwendet. Einige Lightsail-Vorlagen unterstützen derzeit kein IPv6-onlyNetzwerk. Informationen dazu, welche Vorlagen IPv6-onlyNetzwerke unterstützen, finden Sie unter Wählen Sie ein Amazon Lightsail-Instance-Image.

   Ein Plan umfasst auch niedrige, vorhersehbare Kosten und eine Maschinenkonfiguration (RAM, SSD, vCPU) sowie Datenübertragung.

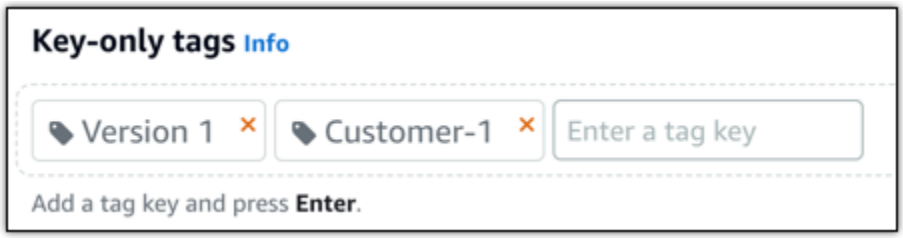
   > **Note**
   >
   > Einige Instance-Preismodelle sind für manche Vorlagen nicht verfügbar. Sie können z. B. die beiden günstigsten Preismodelle nicht mit der SQL Server Express-Vorlage verwenden. Sie müssen mindestens das Preismodell mit 2 GB RAM und 50 GB SSD verwenden oder eines der teureren Preismodelle auswählen.
7. Geben Sie einen Namen für Ihre Instance ein.

   Ressourcennamen:

- Muss in jedem AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
- Muss zwischen 2 und 255 Zeichen enthalten.
- Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
- Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

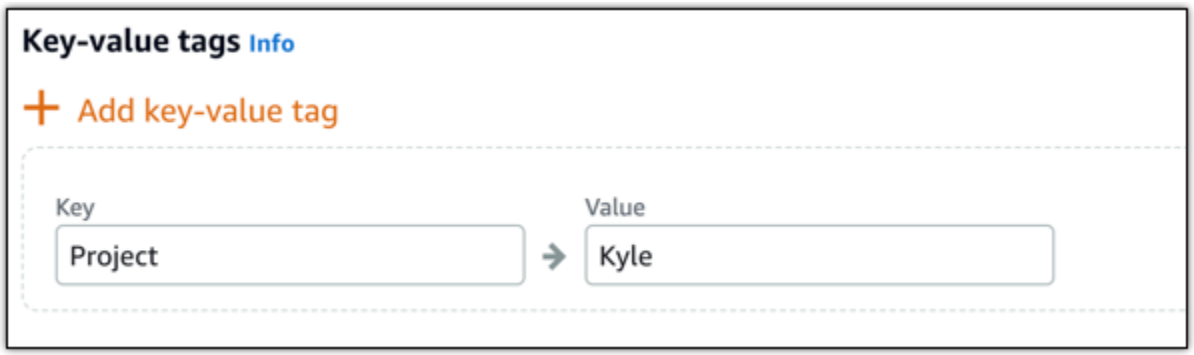
8. Wählen Sie eine der folgenden Optionen, um Ihrer Instance Tags hinzuzufügen:

   - Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.

   - Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

     Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.

> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

9. Wählen Sie Create instance (Instance erstellen).

So erstellen Sie eine Instance mit der AWS CLI

1. Falls noch nicht erfolgt, installieren und konfigurieren Sie die AWS CLI.

   Weitere Informationen finden Sie unter Konfigurieren der AWS Command Line Interface für die Arbeit mit Amazon Lightsail.
2. Öffnen Sie eine Eingabeaufforderung oder ein Terminal-Fenster.
3. Wenn Sie dies noch nicht getan haben, konfigurieren Sie die AWS CLI mit `aws configure` und wählen Sie die aus, AWS-Region in der Sie Ihre Lightsail-Ressourcen erstellen möchten.
4. Geben Sie den folgenden AWS CLI Befehl ein, um eine Windows Server 2016-Instance für 40 USD pro Monat zu erstellen, die in der Region Ohio ausgeführt wird:

   ```
   aws lightsail create-instances --instance-names InstanceName --availability-
   zone us-east-2a --blueprint-id windows_server_2016_2017_09_13 --bundle-id
    medium_win_1_0
   ```

   Ersetzen Sie im Befehl durch *InstanceName* den Namen Ihrer neuen Instance.

   Wenn der Befehl erfolgreich ausgeführt wurde, sehen Sie die folgende Ausgabe von der AWS CLI:

   ```
   {
       "operations": [
           {
               "status": "Started",
               "resourceType": "Instance",
               "isTerminal": false,
               "statusChangedAt": 1508086226.4,
               "location": {
                   "availabilityZone": "us-east-2a",
   ```

```
                "regionName": "us-east-2"
            },
            "operationType": "CreateInstance",
            "resourceName": "my-windows-instance",
            "id": "344acdc8-f9c4-4eda-8232-12345EXAMPLE",
            "createdAt": 1508086225.467
        }
    ]
}
```

> **Note**
>
> Um eine Liste der verfügbaren Vorlagen anzuzeigen, verwenden Sie den Befehl get-blueprints. Um eine Liste der verfügbaren Pakete anzuzeigen, verwenden Sie den Befehl get-bundles. Erfahren Sie mehr über das Abrufen des Passworts für Ihre Instance mit dem get-instance-access-details Befehl .

Herstellen einer Verbindung zu Ihrer Instance

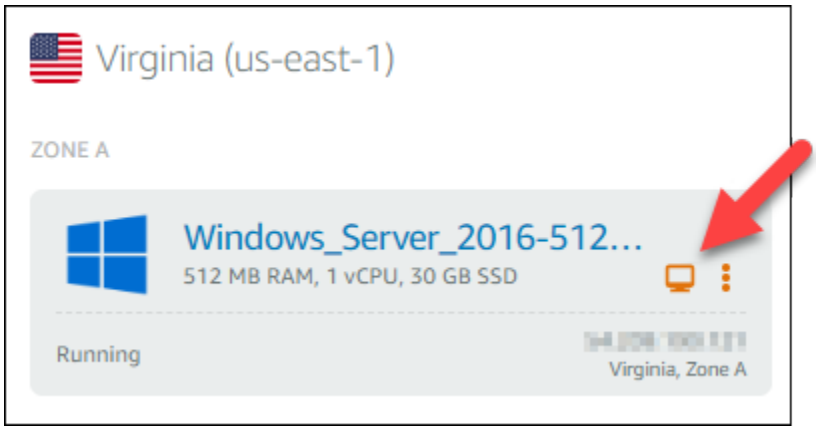
Sobald Sie Ihre Windows Server-basierte Lightsail-Instance erstellt haben, können Sie eine Verbindung zu ihr entweder über den browserbasierten RDP-Client oder den Remote-Desktop-Client Ihrer Wahl herstellen.

> **Note**
>
> Nachdem Sie Ihre Instance erstellt haben, kann es bis zu 15 Minuten dauern, bevor Sie eine Verbindung mit ihr herstellen können.

So stellen Sie eine Verbindung mit dem browserbasierten Lightsail-RDP-Client her

1.
> **Note**
>
> Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um SSH oder RDP über IPv6 in Ihre Instance zu übertragen. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

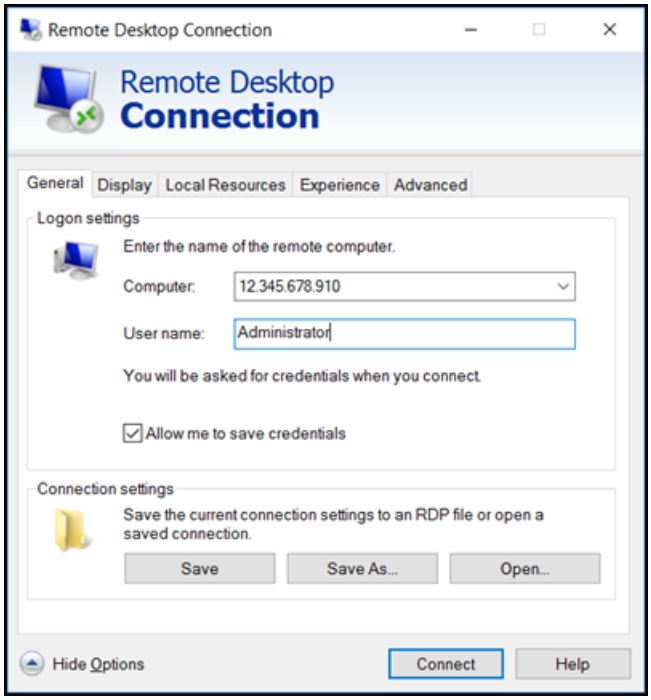
Klicken Sie auf der Startseite auf das Symbol Connect using RDP (Mit RDP verbinden) neben der Instance.



2. Alternativ können Sie über das Kontextmenü oder die Instance-Management-Seite eine Verbindung zu der Instance herstellen.

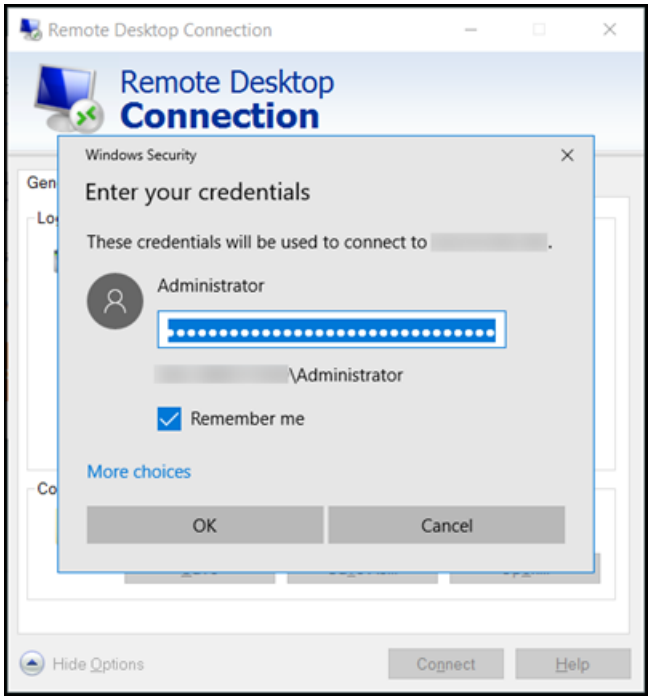
So stellen Sie eine Verbindung über einen eigenen RDP-Client her

1. Um Ihre IP-Adresse zu erhalten, gehen Sie zur Lightsail-Startseite.
2. Kopieren Sie die IP-Adresse in die Zwischenablage.
3. Öffnen Sie einen RDP-Client unter Windows zum Beispiel Remote Desktop Connection (Remote-Desktop-Verbindung).
4. Fügen Sie die IP-Adresse in das Feld Computer ein.
5. Wählen Sie Show Options (Optionen anzeigen) aus und geben Sie `Administrator` als User name (Benutzernamen) ein.



6. Wählen Sie Connect aus.
7. Um Ihr Passwort zu erhalten, rufen Sie die Instance-Verwaltungsseite in Lightsail auf.

   Sie können zur Instance-Verwaltungsseite gelangen, indem Sie auf der Lightsail-Startseite den Namen Ihrer Instance auswählen (oder im Verknüpfungsmenü Verwalten auswählen).
8. Klicken Sie auf Show default password (Standardpasswort anzeigen).
9. Kopieren Sie das Standardpasswort in die Zwischenablage.
10. Fügen Sie Ihr Passwort im Feld Remote Desktop Connection (Remote-Desktop-Verbindung) ein und wählen Sie Remember me (Passwort speichern) aus, um dieses Dialogfeld in Zukunft zu unterdrücken.



11. Wählen Sie OK aus.
12. Klicken Sie auf Don't ask me again for connections to this computer (Verbindungen zu diesem Computer erlauben) und auf Yes (Ja).

Instances (virtuelle private Server) in Amazon Lightsail

Ihre Lightsail-Instance ist ein virtueller privater Server (auch als virtuelle Maschine bezeichnet). Wenn Sie Ihre Instance erstellen, wählen Sie ein Abbild aus, das ein Betriebssystem (OS) hat. Sie können auch ein Instance-Image wählen, das eine Anwendung oder einen Entwicklungs-Stack enthält, einschließlich des Basis-Betriebssystems.

Eine vollständige Liste der Betriebssysteme, Anwendungen und Entwicklungs-Frameworks finden Sie unter Auswählen eines Lightsail-Instance-Images.

Weitere Informationen über Instances finden Sie in den folgenden Themen:

Themen

Erstellen einer Lightsail-Instance

Sie können innerhalb von Sekunden eine Lightsail-Instance erstellen, auch als Virtual Private Server (VPS) bezeichnet, auf der eine Anwendung wie WordPress oder ein Entwicklungs-Stack wie LAMP ausgeführt wird. Nachdem Ihre Instance gestartet wurde, können Sie über SSH eine Verbindung zu ihr herstellen, ohne Lightsail zu verlassen. Das geht so:

1. Wählen Sie auf der Website Create instance (Instance erstellen).
2. Wählen Sie einen Standort für Ihre Instance (eine AWS-Region und eine Availability Zone).

   Wählen Sie Verändern von AWS-Region und Availability Zone aus, um den Speicherort für die Instance zu ändern.

3. Optional können Sie die Availability Zone wechseln.

   Wählen Sie eine Availability Zone aus der Dropdown-Liste.

4. Wählen Sie eine Anwendung (Apps + OS) oder ein Betriebssystem (OS Only (Nur OS)) aus.

   Weitere Informationen zu Lightsail-Instance-Images finden Sie unter Auswählen eines Amazon Lightsail-Instance-Images.

5. Wählen Sie Ihren Instance-Plan aus.

   Wählen Sie aus, ob Ihre Instance Dual-Stack-Netzwerke (IPv4 und IPv6) oder IPv6-onlyNetzwerke verwendet. Einige Lightsail-Vorlagen unterstützen derzeit kein IPv6-onlyNetzwerk. Informationen dazu, welche Vorlagen IPv6-onlyNetzwerke unterstützen, finden Sie unter Wählen Sie ein Amazon Lightsail-Instance-Image.

   Sie können den Lightsail-Plan 3,50 USD einen Monat lang kostenlos (bis zu 750 Stunden) testen. Wir fügen Ihrem Konto einen kostenlosen Monat hinzu. Erfahren Sie mehr auf unserer Lightsail-Preisgestaltungsseite.

   > **Note**
   >
   > Im Rahmen des AWS kostenlosen Kontingents für können Sie kostenlos mit Amazon Lightsail für ausgewählte Instance-Pakete beginnen. Weitere Informationen finden Sie unter AWS Kostenloses Kontingent auf der Seite Amazon Lightsail – Preise.

6. Geben Sie einen Namen für Ihre Instance ein.

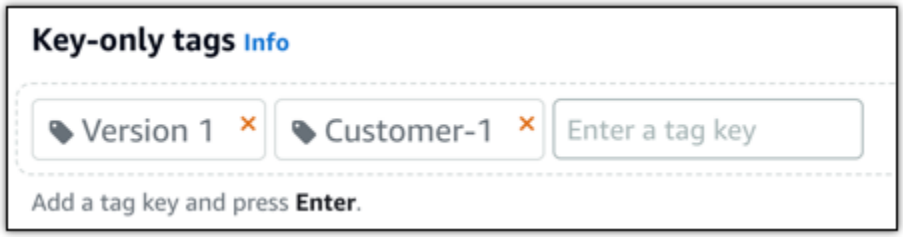
   Ressourcennamen:

   - Muss in jedem AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

7. Wählen Sie eine der folgenden Optionen, um Ihrer Instance Tags hinzuzufügen:

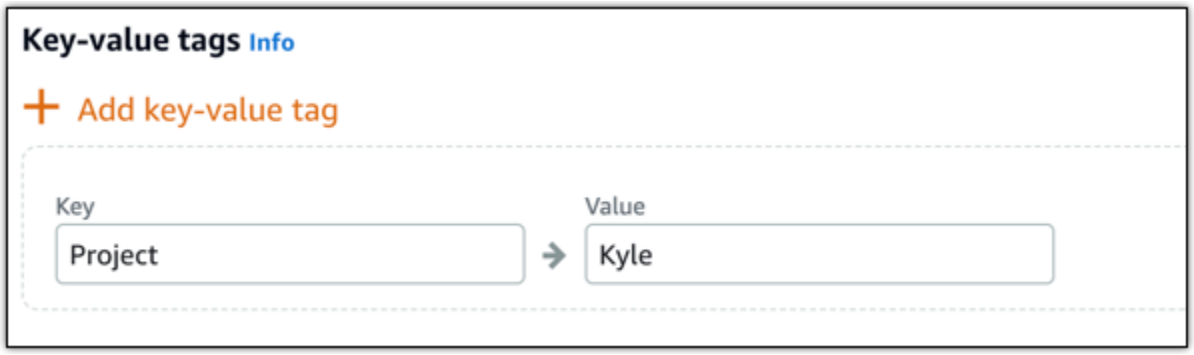
   - Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern),

wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.



- Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

  Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.



> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

8. Wählen Sie Create instance (Instance erstellen).

   Informationen zu erweiterten Erstellungsoptionen finden Sie unter Verwenden eines Startskripts zum Konfigurieren Ihrer Amazon Lightsail-Instance beim Start oder Einrichten von SSH für Ihre Linux/Unix-basierten Instances.

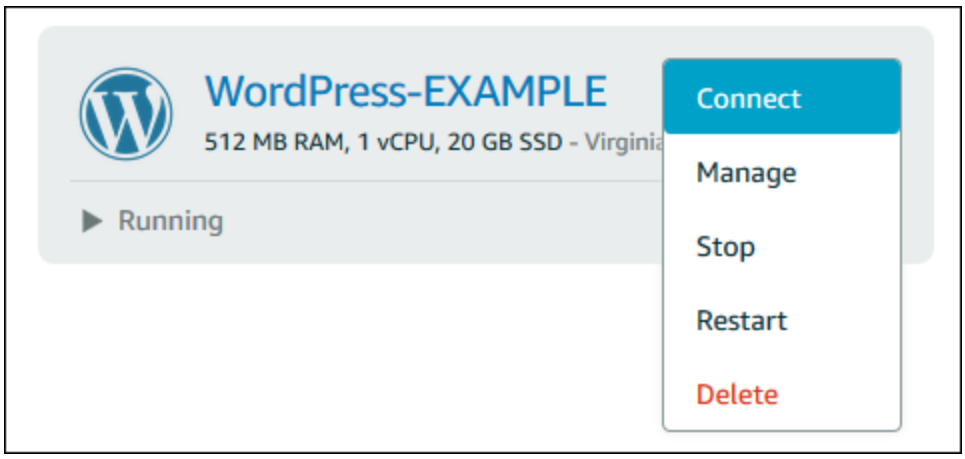
Innerhalb weniger Minuten ist Ihre Lightsail-Instance bereit und Sie können eine Verbindung über SSH herstellen, ohne Lightsail zu verlassen!

Eine Verbindung mit Ihrer Instance herstellen

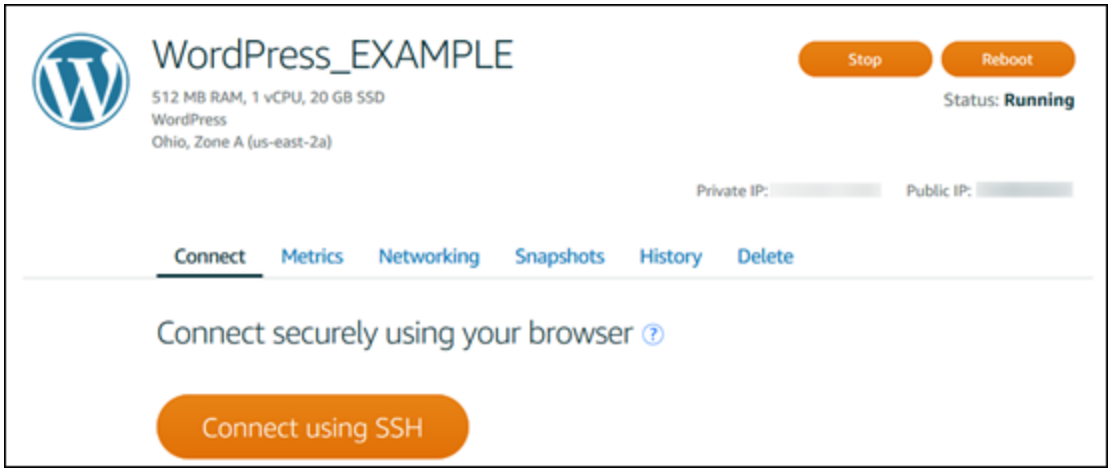
1.

> **Note**
>
> Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um SSH oder RDP über IPv6 in Ihre Instance zu übertragen. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

Wählen Sie auf der Lightsail-Startseite das Menü rechts neben dem Namen Ihrer Instance und dann Verbinden aus.

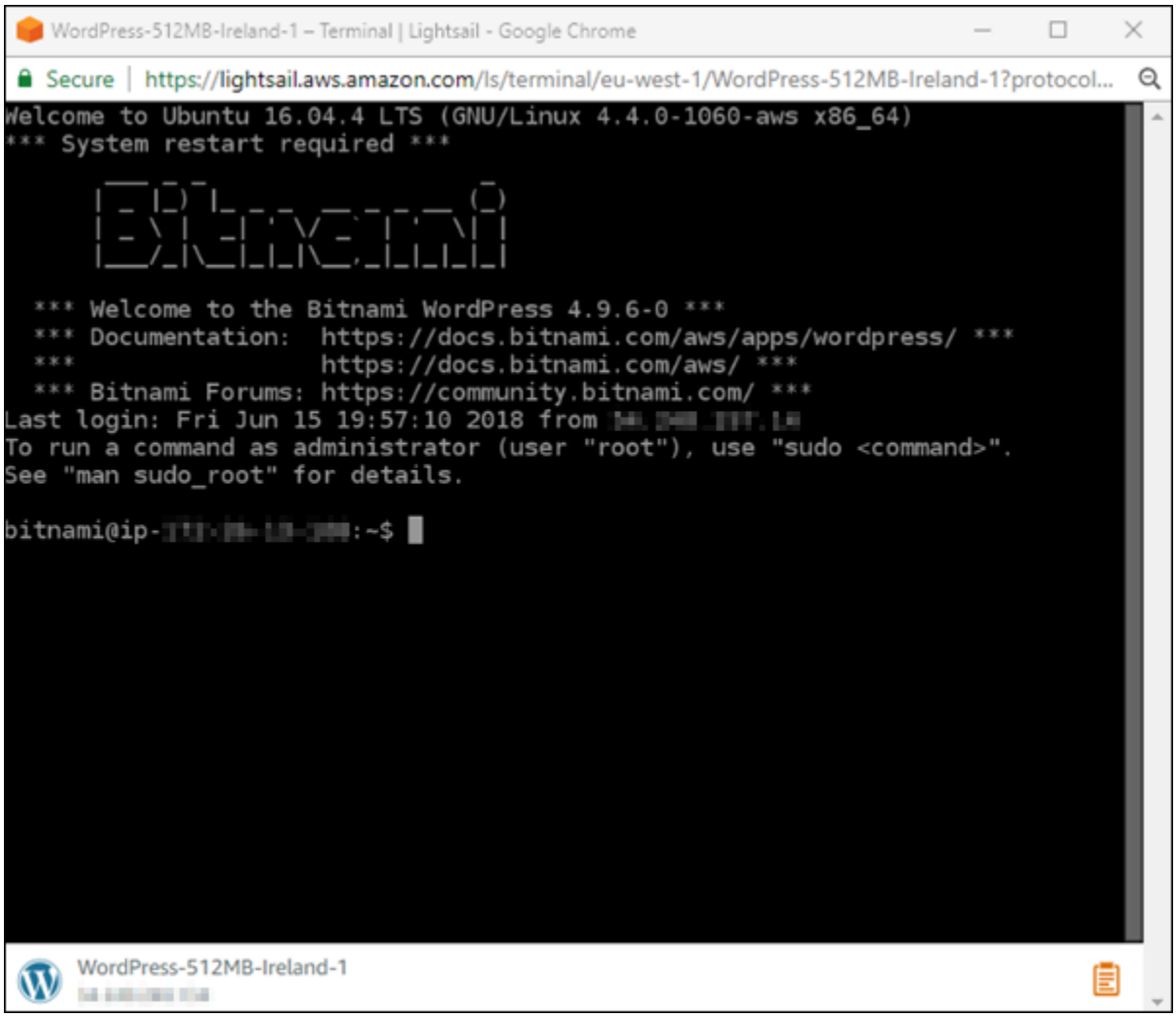


Alternativ können Sie die Verwaltungsseite für Ihre Instance öffnen und dort auf die Registerkarte Connect (Verbinden) gehen.



> **Note**
>
> Wenn Sie über einen SSH-Client wie PuTTY eine Verbindung zu Ihrer Instance herstellen möchten, können Sie die folgenden Schritte ausführen: PuTTY einrichten, um eine Verbindung zu Ihrer Lightsail-Instance herzustellen.

2. Sie können jetzt Befehle in das Terminal eingeben und Ihre Lightsail-Instance verwalten, ohne einen SSH-Client einzurichten.



Nächste Schritte

Nachdem Sie eine Verbindung mit der Instance eingerichtet haben, sind Ihre nächsten Schritte davon abhängig, wie Sie sie verwenden möchten. Beispielsweise:

- the section called “WordPress” , wenn Sie einen Blog erstellen.
- Erstellen Sie eine statische IP-Adresse für Ihre Instance, damit sie bei jedem Neustart Ihrer Lightsail-Instance dieselbe IP-Adresse beibehält.
- Erstellen eines Snapshots Ihrer Instance als Sicherung.

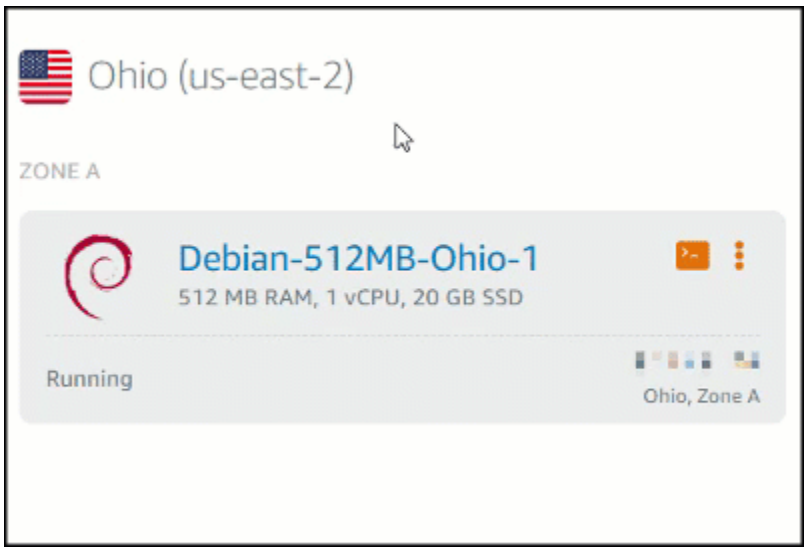
Löschen einer Lightsail-Instance

Wenn Sie eine Instance nicht mehr benötigen, können Sie sie über die Amazon Lightsail-Konsole oder die AWS Command Line Interface (AWS CLI) löschen. Sobald die Instance gelöscht wurde, fallen keine weiteren Kosten für sie mehr an. Ressourcen, die an die gelöschte Instance angehängt sind, wie statische IPs und Snapshots, verursachen jedoch weiterhin Kosten, bis Sie sie löschen.

> **Note**
>
> Gelöschte Instances können nicht wiederhergestellt werden. Erstellen Sie vor dem Löschen einen Snapshot einer Instance, wenn Sie die Daten in der Instance möglicherweise zu einem späteren Zeitpunkt benötigen. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Linux- oder Unix-Instance oder Erstellen eines Snapshots Ihrer Windows-Server-Instance.

Löschen einer Instance von der Startseite der Lightsail-Konsole

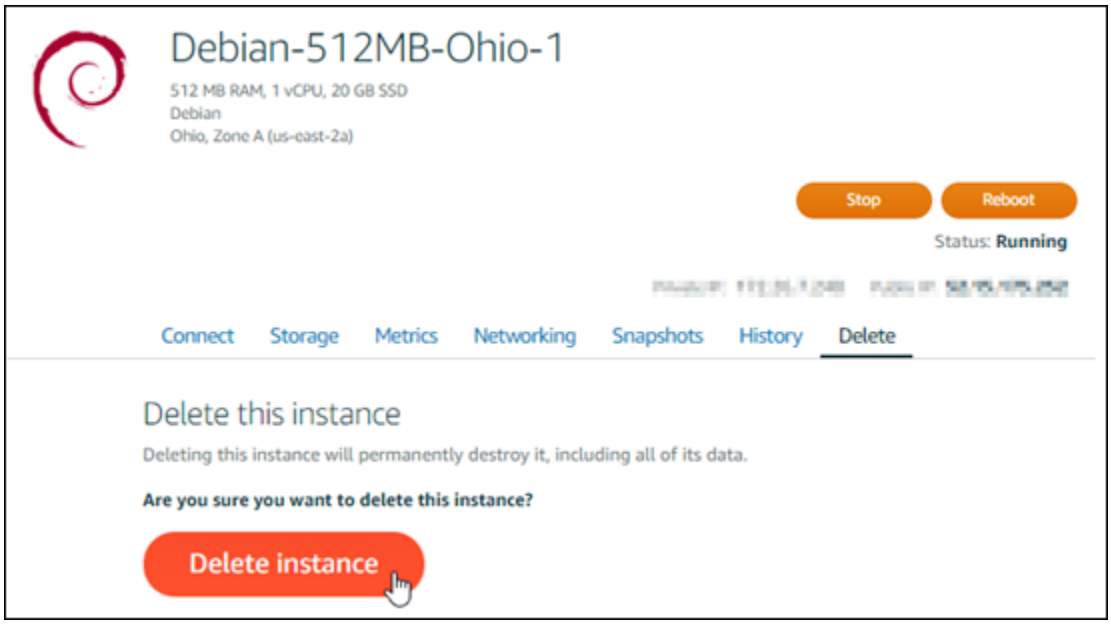
1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie für die zu löschende Instance das Aktionsmenü-Symbol (⋮) und dann Delete (Löschen).



3. Wählen Sie Yes (Ja) zum Bestätigen der Löschung.

Löschen einer Instance von der Instance-Verwaltungsseite der Lightsail-Konsole

1. Wählen Sie auf der Startseite der Lightsail-Konsole die Instance aus, die Sie löschen möchten.
2. Wählen Sie die Registerkarte Delete (Löschen) aus, und wählen Sie dann Delete Instance (Löschen).



3. Wählen Sie Yes (Ja) zum Bestätigen der Löschung.

Löschen einer Instance mithilfe der AWS CLI

1. Erfüllen Sie die folgenden Voraussetzungen, wenn dies noch nicht geschehen ist:

   a. Installieren Sie den AWS CLI. Weitere Informationen finden Sie unter Installieren der AWS CLI.

   b. Konfigurieren Sie AWS CLI. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI.

2. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster und geben Sie dann den folgenden Befehl ein, um den Namen der Instance zu erhalten, die Sie löschen möchten:

   ```
   aws lightsail get-instances
   ```

   Sie sollten ähnliche Ergebnisse wie nachfolgend zu sehen:

3. Wählen Sie und kopieren Sie den Namen der Instance, die Sie löschen möchten, damit Sie ihn im nächsten Schritt verwenden können.

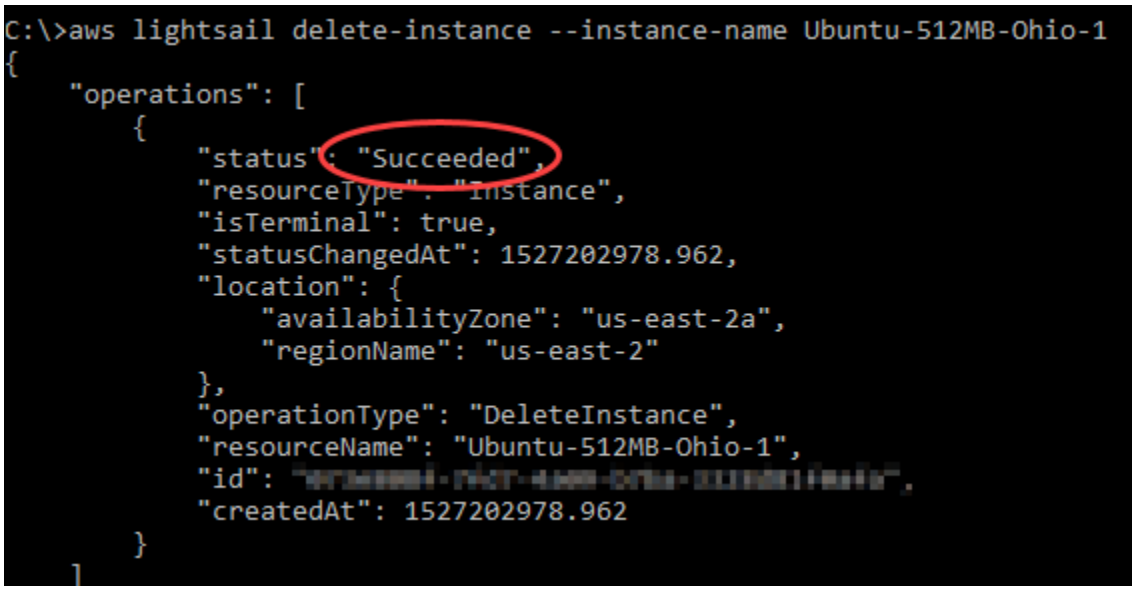
> **Note**
>
> Wenn die zu löschende Instance nicht angezeigt wird, stellen Sie sicher, dass Ihre AWS CLI für die AWS-Region konfiguriert ist, in der sich die Instance befindet. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI.

4. Geben Sie den folgenden Befehl ein, um die Instance zu löschen:

```
aws lightsail delete-instance --instance-name InstanceName
```

Ersetzen Sie im Befehl *InstanceName* durch den Namen der Instance.

Wenn das Löschen erfolgreich war, sollten Sie eine Bestätigung ähnlich der folgenden sehen:



> **Note**
>
> Wenn das Löschen nicht erfolgreich ist, sollten Sie eine Fehlermeldung erhalten. Stellen Sie sicher, dass Sie den genauen Namen der Instance kopiert und eingefügt haben und versuchen Sie es erneut.

Nächste Schritte

Nachdem Sie eine Instance gelöscht haben, bleiben eine statische IP, Snapshots, Blockspeicher-Datenträger und Load Balancer, die der Instance zugeordnet sind, weiterhin in Lightsail aufrecht und verursachen zusätzliche Kosten. Weitere Informationen zum Löschen dieser Ressourcen finden Sie in den folgenden Artikeln:

- Eine statische IP löschen
- Löschen eines Snapshots
- Trennen und Löschen eines Blockspeicherdatenträgers

- Löschen eines Load Balancers

Wählen Sie ein Amazon Lightsail-Instance-Image

Lightsail bietet Ihnen mehrere Optionen zum Erstellen Ihres virtuellen privaten Servers. Dieses Thema hilft Ihnen bei der Entscheidung, welches Betriebssystem (BS), welche Anwendung und welcher Entwicklungs-Stack für Ihr Projekt am besten geeignet ist. Wir organisieren die Anwendungen nach Funktionsbereich (z. B. CMS und E-Commerce).

Vergleichen von Plattformen

Lightsail hat zwei Plattformen zur Auswahl: Linux/UNIX-basierte oder Windows-basierte Plattformen. Wenn Sie sich bereits für eine Anwendung entschieden haben, haben Sie wahrscheinlich schon eine Plattform für das Betriebssystem ausgewählt. Sie können für den Anfang eine der folgenden Optionen auswählen:

- Erste Schritte mit Linux-/Unix-basierten Instances
- Erste Schritte mit Windows-basierten Instances

Betriebssysteme vergleichen

Lightsail hat mehrere Betriebssysteme zur Auswahl.

Windows Server 2022

> Lightsail, auf dem Windows Server ausgeführt wird, ist eine schnelle und zuverlässige Umgebung für die Bereitstellung von Anwendungen mithilfe der Microsoft Web Platform. Mit Lightsail können Sie jede kompatible Windows-basierte Lösung auf der leistungsstarken, zuverlässigen und kostengünstigen Computerplattform ausführen. AWS Cloud Häufige Windows-Anwendungsfälle umfassen Enterprise-Windows-basiertes Anwendungshosting, Website- und Webservice-Hosting, Datenverarbeitung, verteiltes Testen, ASP.NET-Anwendungshosting und jede andere Windows-Software, die Anwendungen erfordert. Informationen zum Ende des Supports finden Sie auf der Microsoft-Website.
>
> Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.
>
> Weitere Informationen über das Windows-Server-2022-Image

Windows Server 2019

Lightsail, auf dem Windows Server ausgeführt wird, ist eine schnelle und zuverlässige Umgebung für die Bereitstellung von Anwendungen mithilfe der Microsoft Web Platform. Mit Lightsail können Sie jede kompatible Windows-basierte Lösung auf der leistungsstarken, zuverlässigen und kostengünstigen AWS-Cloud-Computing-Plattform ausführen. Häufige Windows-Anwendungsfälle umfassen Enterprise-Windows-basiertes Anwendungshosting, Website- und Webservice-Hosting, Datenverarbeitung, verteiltes Testen, ASP.NET-Anwendungshosting und jede andere Windows-Software, die Anwendungen erfordert. Informationen zum Ende des Supports finden Sie auf der Microsoft-Website.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Weitere Informationen über das Windows-Server-2019-Image

Windows Server 2016

Lightsail, auf dem Windows Server ausgeführt wird, ist eine schnelle und zuverlässige Umgebung für die Bereitstellung von Anwendungen mithilfe der Microsoft Web Platform. Mit Lightsail können Sie jede kompatible Windows-basierte Lösung auf der leistungsstarken, zuverlässigen und kostengünstigen AWS-Cloud-Computing-Plattform ausführen. Häufige Windows-Anwendungsfälle umfassen Enterprise-Windows-basiertes Anwendungshosting, Website- und Webservice-Hosting, Datenverarbeitung, verteiltes Testen, ASP.NET-Anwendungshosting und jede andere Windows-Software, die Anwendungen erfordert. Informationen zum Ende des Supports finden Sie auf der Microsoft-Website.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Weitere Informationen über das Windows Server 2016-Image

Amazon Linux 2023

Amazon Linux 2023 (AL2023) ist die nächste Generation von Amazon Linux und ideal für allgemeine Workloads in AWS. AL2023 wird fünf Jahre lang unterstützt, nachdem es allgemein verfügbar wurde. AL2023 ist an eine bestimmte Version des Paket-Repositorys von Amazon Linux gebunden, sodass Sie die Kontrolle darüber haben, wie und wann Sie Updates durchführen. AL2023 bietet auch die Möglichkeit, häufige Updates zu erhalten, und verfügt über Funktionen, mit denen Sie Ihre Compliance-Anforderungen erfüllen können.

Lightsail Lightsail-Instances, die von AL2023 aus gestartet werden, wird Instance Metadata Service Version 2 (IMDSv2) standardmäßig durchgesetzt. Weitere Informationen finden Sie unter Funktionsweise von Instance-Metadatenservice Version 2.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Weitere Informationen über Amazon Linux 2023.

Amazon Linux 2

Amazon Linux 2 ist die vorherige Generation von Amazon Linux, einem Linux-Serverbetriebssystem von AWS. Es bietet eine stabile, sichere und leistungsstarke Ausführungsumgebung, um Cloud- und Unternehmensanwendungen zu entwickeln und auszuführen. Mit Amazon Linux 2 erhalten Sie eine Anwendungsumgebung, die langfristige Unterstützung bietet und Zugriff auf die neuesten Innovationen in Linux bietet. Wird für Amazon Linux 2 wird ohne Zusatzkosten angeboten. Informationen zum Ende des Supports finden Sie unter Amazon Linux 2 – Häufig gestellte Fragen.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Erfahren Sie mehr über Amazon Linux 2.

AlmaLinux OS 9

AlmaLinux OS 9 ist eine Open-Source-Linux-Distribution für Unternehmen, die sich im Besitz der Community befindet und von der Community verwaltet wird und für immer kostenlos ist. Sie konzentriert sich auf langfristige Stabilität und bietet eine robuste Plattform in Produktionsqualität. AlmaLinux ist mit RHEL® und Pre-Stream CentOS kompatibel. Informationen zum Ende des Supports finden Sie auf der AlmaLinux OS Foundation-Website.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Erfahren Sie mehr über OS 9 AlmaLinux

CentOS 7

> **Important**
>
> CentOS 7 wird am 30. Juni 2024 das Ende der Lebensdauer (EOL) erreichen. Am oder nach dem 30. Juni 2024 können Sie keine neuen Lightsail-Instanzen mit diesem Blueprint erstellen. Weitere Informationen finden Sie auf der CentOS-Website.

CentOS ist eine Linux-Distribution, die eine kostenlose, von Unternehmen genutzte, von der Community unterstützte Computerplattform anbietet, die funktional mit ihrer vorgelagerten Quelle

Red Hat Enterprise Linux kompatibel ist. Informationen zum Ende des Supports finden Sie auf der Red-Hat-Website.

Weitere Informationen zu CentOS 7.

CentOS Stream 9

CentOS Stream 9 ist die nächste Hauptversion der CentOS-Stream-Distribution. CentOS Stream 9 ist eine fortlaufend ausgelieferte Distribution, die der Entwicklung von Red Hat Enterprise Linux (RHEL) dicht auf den Fersen ist und als Mittelweg zwischen Fedora Linux und RHEL positioniert ist. Sie wurde so konzipiert, dass sie funktional mit RHEL kompatibel ist und eine stabile, vorhersehbare, verwaltbare und reproduzierbare Linux-Umgebung bietet. Informationen zum Ende des Supports finden Sie auf der CentOS-Website.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Weitere Informationen zu CentOS Stream.

Debian 10, 11 und 12

> **Important**
>
> Debian 10 wird am 30. Juni 2024 das Ende der langfristigen Unterstützung erreichen. Am oder nach dem 30. Juni 2024 können Sie keine neuen Lightsail-Instanzen mit diesem Blueprint erstellen.

Debian ist ein kostenloses Betriebssystem, das von Tausenden von Freiwilligen aus der ganzen Welt entwickelt wurde, die über das Internet zusammenarbeiten. Die wichtigsten Stärken des Debian-Projekts sind seine Freiwilligenbasis, sein Engagement für den Debian-Gesellschaftsvertrag und kostenlose Software sowie sein Engagement, das bestmögliche Betriebssystem bereitzustellen. Diese neue Version ist ein weiterer wichtiger Schritt in diese Richtung. Informationen zum Ende des Supports finden Sie auf der Debian-Website.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Weitere Informationen über Debian.

FreeBSD 13

FreeBSD ist ein Betriebssystem, das für Server, Desktops und eingebettete Systeme verwendet wird. FreeBSD ist von BSD abgeleitet, der UNIX-Version, die an der University of California,

Berkeley, entwickelt wurde. Es wird seit mehr als 30 Jahren von einer großen Community stetig weiterentwickelt. Die Netzwerk-, Sicherheits-, Speicher- und Überwachungsfunktionen von FreeBSD, einschließlich der pf-Firewall, der Capsicum- und CloudABI-Frameworks und des ZFS-Dateisystems sowie des Frameworks „DTrace Dynamic Tracing“ machen FreeBSD zur Plattform der Wahl für viele der meistbesuchten Websites sowie die meisten eingebetteten Netzwerk- und Speichersysteme. Informationen zum Ende des Supports finden Sie auf der FreeBSD-Website.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Weitere Informationen über FreeBSD.

openSUSE 15

Die openSUSE-Distribution ist eine stabile, benutzerfreundliche und vollständige Mehrzweck-Linux-Distribution. Es ist für Benutzer und Entwickler vorgesehen, die auf dem Desktop oder Server arbeiten. Es ist ideal geeignet für Anfänger, erfahrene Benutzer und Ultra-Nerds gleichermaßen, kurz gesagt, es ist perfekt für alle! Informationen zum Ende des Supports finden Sie auf der openSUSE-Website.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Weitere Informationen über openSUSE.

Ubuntu 18, 20 und 22

> **Important**
>
> Ubuntu 18.04 hat am 31. Mai 2023 das Ende des Standard-Supports erreicht. Am oder nach dem 31. Mai 2024 können Sie keine neuen Lightsail-Instanzen mit diesem Blueprint erstellen. Weitere Informationen finden Sie auf der Ubuntu-Website.

Ubuntu Server ist ein auf Debian basierendes Linux-Betriebssystem für virtuelle Server. Eine Standardinstallation von Ubuntu enthält eine breite Palette von Software LibreOffice, darunter Firefox, Thunderbird und Transmission. Sie können viele zusätzliche Softwarepakete installieren, z. B. Evolution, GIMP, Pidgin und Synaptic. Dazu verwenden Sie das auf APT basierende Tool zur Paketverwaltung (`apt-get`). Informationen zum Ende des Supports finden Sie auf der Ubuntu-Website.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Weitere Informationen über Ubuntu.

Vergleichen von Datenbankanwendungen

Die folgenden Datenbankanwendungen sind in Lightsail verfügbar:

SQL Server 2022 Express

SQL Server Express ist ein relationales Datenbankverwaltungssystem, das kostenlos heruntergeladen, verteilt und verwendet werden kann. Es besteht aus einer Datenbank, die speziell auf eingebettete und kleinere Anwendungen ausgerichtet ist. Dieses Lightsail-Image läuft auf einem Basisbetriebssystem von Windows Server 2022.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Weitere Informationen zum SQL-Server-2022-Express-Image

SQL Server 2019 Express

SQL Server Express ist ein relationales Datenbankverwaltungssystem, das kostenlos heruntergeladen, verteilt und verwendet werden kann. Es besteht aus einer Datenbank, die speziell auf eingebettete und kleinere Anwendungen ausgerichtet ist. Dieses Lightsail-Image läuft auf einem Basisbetriebssystem von Windows Server 2022.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Weitere Informationen zum SQL-Server-2019-Express-Image

SQL Server 2016 Express

SQL Server Express ist ein relationales Datenbankverwaltungssystem, das kostenlos heruntergeladen, verteilt und verwendet werden kann. Es besteht aus einer Datenbank, die speziell auf eingebettete und kleinere Anwendungen ausgerichtet ist. Dieses Lightsail-Image läuft auf einem Basisbetriebssystem von Windows Server 2016.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Weitere Informationen zum SQL-Server-2016-Express-Image

CMS-Anwendungen vergleichen

Die folgenden Content Management System (CMS) -Anwendungen sind in Lightsail verfügbar:

WordPress zertifiziert von Bitnami

Bitnami WordPress ist ein vorkonfiguriertes ready-to-use Image für die Ausführung WordPress auf Lightsail. WordPress ist eine beliebte Web-Publishing-Plattform zum Erstellen von Blogs und Websites. Sie können sie unter Verwendung einer großen Auswahl an Designs, Erweiterungen, Plugins und Widgets anpassen.

WordPress bietet ein vollständiges Themensystem, mit dem Sie das Erscheinungsbild Ihrer Website mit wenigen Klicks ändern können. Sie können auch bestehende kostenlose oder kommerzielle WordPress Themes verwenden. WordPress entspricht in vollem Umfang den Standards des W3C.

Erfahren Sie mehr über die Bitnami-Anwendung WordPress .

WordPress Multisite, zertifiziert von Bitnami

WordPress Multisite ermöglicht es Administratoren, mehrere Websites von derselben Instanz aus zu hosten und zu verwalten. WordPress Diese Websites können alle eindeutige Domainnamen haben und können von ihren Besitzern angepasst werden, während sie Elemente wie Themen und Plug-ins gemeinsam nutzen, die vom Server-Administrator zur Verfügung gestellt werden. Aktualisierungen können für alle Websites gleichzeitig übertragen werden, so kann sichergestellt werden, dass sie immer sicher und geschützt sind.

WordPress Multisite eignet sich hervorragend für Organisationen wie Universitäten, Unternehmen und Agenturen, die es vielen Menschen ermöglichen müssen, ihre eigenen Websites zu hosten und gleichzeitig die Gesamtkontrolle einem zentralen Administrator zu übertragen.

Erfahren Sie mehr über die Bitnami WordPress Multisite-Anwendung.

cPanel und WebHost Manager (WHM)

cPanel & WHM ist eine Suite von Tools, die für das Linux-Betriebsystem entwickelt wurde und die Ihnen die Möglichkeit gibt, Web-Hosting-Aufgaben über eine einfache grafische Benutzeroberfläche zu automatisieren. Ihr Ziel ist es, die Verwaltung von Servern für Sie zu erleichtern und Websites für Ihre Kunden zu verwalten.

Weitere Informationen über cPanel & WHM.

PrestaShop verpackt von Bitnami

PrestaShop ist eine der produktivsten E-Commerce-Lösungen der Welt. Es ist freie und Open-Source-Software, mit einer Community von über 1 Million aktiven Mitgliedern. Es wurde entwickelt, um Ihren Online-Shop schnell zum Laufen zu bringen. Es verfügt über ein

vorkonfiguriertes Thema, sodass Sie fast sofort mit dem Verkauf beginnen können, sowie über einen Live-Konfigurator, mit dem Sie das Erscheinungsbild Ihrer Website einfach anpassen können. PrestaShop bietet Unterstützung für mehrere Geschäfte, anpassbare URLs, mehrere Zahlungsgateway-Optionen (einschließlich PayPal Stripe) und Marktplatzintegration mit Amazon, eBay, Facebook und mehr.

Erfahre mehr über PrestaShop.

Ghost verpackt von Bitnami

Ghost ist eine Veröffentlichungsplattform, die sich für alles von persönlichen Blogs bis hin zu großen Nachrichten-Websites eignet. Der auf Node.js aufbauende moderne Technologie-Stack macht ihn vielseitig und flexibel für Entwickler, die eine Integration in andere Anwendungen und Tools anstreben, bei der gleichzeitig die Benutzerfreundlichkeit für die Ersteller von Inhalten erhalten bleiben soll.

Weitere Informationen über die Bitnami Ghost-Anwendung.

Joomla! verpackt von Bitnami

Bitnami Joomla! ist ein vorkonfiguriertes ready-to-use Image zum Ausführen von Joomla! auf Lightsail. Joomla! ist ein CMS, das Sie für die Entwicklung einer Vielzahl von Websites oder Portalen verwenden können. Dabei handelt es sich unter anderem um Websites für Privatpersonen, Vereine, kleine Unternehmen, gemeinnützige und andere Organisationen.

Joomla! unterstützt außerdem ein Registrierungssystem, mit der Benutzer auch persönliche Optionen konfigurieren können. Authentifizierung ist ein wichtiger Teil der Benutzerverwaltung, und Joomla! unterstützt mehrere Protokolle, einschließlich LDAP, OpenID und andere. Joomla! unterstützt viele verschiedene Sprachen und bietet Anleitungen für ihre Verwendung für die Website und die Administration. Der Banner Manager erleichtert auch das Einrichten und Verwalten von Bannern auf Ihrer Website. Sie können Metriken verfolgen, unter anderem die Einrichtung von Impressionszahlen, speziellen URLs und vielem anderen mehr.

Weitere Informationen über die Bitnami Joomla!-Anwendung.

Joomla! verpackt von Bitnami

Bitnami Drupal ist ein vorkonfiguriertes ready-to-use Image für die Ausführung von Drupal auf Lightsail. Drupal ist eine Content-Management-Plattform, die es Benutzern ermöglicht, auf ganz einfache Weise Inhalt zu veröffentlichen, zu verwalten und zu organisieren. Es wird für Community Web-Portale, Diskussion-Websites, Unternehmenswebsites und anderes verwendet. Sie können Drupal ganz einfach erweitern, indem Sie Module einfügen. Drupal ist auf höchste Leistung

ausgelegt, skalierbar auf viele Server, und unterstützt eine einfache Integration mit REST, JSON, SOAP und anderen Formaten.

Es gibt Tausende von kostenlosen Add-on-Modulen und Designs für Drupal. Drupal ist auch in verschiedenen Sprachen verfügbar.

Weitere Informationen über die Bitnami Drupal-Anwendung.

Vergleichen Sie Anwendungs-Stacks und Server

Lightsail verfügt über fünf Anwendungsstapel und Server für eine Vielzahl von Entwicklungsprojekten. Jedes Image verwendet Linux/Unix (Ubuntu) als Basis-Betriebssystem.

LAMP Stack (PHP 8) verpackt von Bitnami

Der Bitnami LAMP-Stack vereinfacht die Entwicklung und Bereitstellung von PHP-Anwendungen. Es enthält ready-to-run Versionen von Apache, MySQL, PHP und auch die andere Software phpMyAdmin, die zum Ausführen jeder dieser Komponenten erforderlich ist. Der Bitnami LAMP-Stack ist vollständig integriert und konfiguriert, sodass Sie mit der Entwicklung Ihrer Anwendung beginnen können, sobald Sie Ihre Instanz in Lightsail erstellt haben. Der Bitnami LAMP-Stack wird regelmäßig aktualisiert, um sicherzustellen, dass Sie immer Zugriff auf die neuesten stabilen Versionen für jede Paket-Komponente haben.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Weitere Informationen über den Bitnami LAMP-Stack.

Django verpackt von Bitnami

Django ist ein High-Level-Python-Web-Framework, das eine schnelle Entwicklung und ein sauberes, pragmatisches Design fördert. Python ist eine dynamische objektorientierte Programmiersprache, die für viele Arten der Softwareentwicklung verwendet werden kann. Der Bitnami Django Stack vereinfacht die Bereitstellung von Django und seinen Laufzeitabhängigkeiten erheblich und umfasst ready-to-run Versionen von Python, Django, MySQL und Apache.

Weitere Informationen zum Bitnami Django-Stack.

Node.js verpackt von Bitnami

Bitnami Node.js ist ein vorkonfiguriertes ready-to-use Image für die Ausführung von Node.js auf Lightsail. Node.js ist eine Plattform, die auf der JavaScript Runtime von Chrome basiert und die

einfache Erstellung schneller, skalierbarer Netzwerkanwendungen ermöglicht. Es verwendet ein ereignisgesteuertes, nicht blockierende E/A-Modell, mit dem es leicht und effizient wird. Node.js ist gut geeignet für datenintensive Echtzeit-Anwendungen.

Weitere Informationen über den Bitnami Node.js-Stack.

MEAN Stack verpackt von Bitnami

Bitnami MEAN Stack bietet eine vollständige Entwicklungsumgebung für MongoDB und Node.js, die Sie mit einem Klick bereitstellen können. Es enthält die neueste stabile Version von MongoDB, Express, Angular, Node.js, Git, PHP und RockMongo.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Weitere Informationen über den Bitnami MEAN-Stack.

GitLab CE verpackt von Bitnami

Bitnami GitLab Community Edition (CE) ist ein vorkonfiguriertes ready-to-use Image für die Ausführung GitLab auf Lightsail. GitLab ist eine selbst gehostete Git-Verwaltungssoftware, die schnell und sicher ist und auf Ruby on Rails basiert. GitLab CI (ebenfalls enthalten) ist ein Open-Source-Continuous Integration (CI) -Server, der eng in Git und integriert ist GitLab.

GitLab ermöglicht es Ihnen, Ihren Code auf Ihrem eigenen Server zu schützen und Repositorys, Benutzer und Zugriffsberechtigungen zu verwalten. Es ist eigenständig, sodass Sie die Installation auf verschiedenen Servern einfach duplizieren oder verschieben können.

Erfahre mehr über den GitLab Bitnami-Stack.

Nginx (LEMP-Stack) verpackt von Bitnami

Der Bitnami-NGINX-Stack bietet eine vollständige Entwicklungsumgebung für PHP, MySQL und NGINX, die Sie mit einem Klick starten können. Es bündelt auch SQLite phpMyAdmin, FastCGI ImageMagick, Memcache, GD, CURL, PEAR, PECL und andere Komponenten.

NGINX ist ein asynchroner Server. Sein Hauptvorteile ist die Skalierbarkeit. Der NGINX-Stack wird auch als LEMP bezeichnet (Linux, NGINX, MySQL und PHP).

Weitere Informationen über den Bitnami Nginx (LEMP)-Stack.

Plesk Hosting-Stack auf Ubuntu

Mit dem Hosting-Stack von Plesk können Sie Websites und Anwendungen auf Lightsail und AWS erstellen, sichern und ausführen. Dazu gehören all Ihre webbasierten Serververwaltungs- und

Sicherheitstools sowie die WordPress Automatisierung in einer grafischen Benutzeroberfläche. Es vereinfacht die Arbeit von Web-Profis und bietet die Skalierbarkeit, Sicherheit und Performance, die Ihre Kunden benötigen.

Einrichten und Konfigurieren von Plesk.

Erfahren Sie mehr über den Plesk-Stack.

E-Commerce-Anwendungen

Lightsail hat derzeit ein E-Commerce-Anwendungsbild: Magento. Dieses Magento-Image verwendet Linux/Unix (Ubuntu) als Basis-Betriebssystem.

Magento verpackt von Bitnami

Bitnami Magento ist ein vorkonfiguriertes ready-to-use Image für die Ausführung von Magento auf Lightsail. Mit Magento können Sie attraktive, reaktionsschnelle und sichere Websites erstellen. Magento ist eine Feature-reiche, flexible E-Commerce-Lösung, die Transaktionsoptionen, Multistore-Funktionalität, Bonusprogramme, Produktkategorisierung, Shopper-Filter, Werberegeln und vieles andere mehr beinhaltet.

Sie können mit Magento eine weitgehend angepasste E-Commerce-Website erstellen, die Ihre Marke widerspiegelt. Magento lässt sich mit Ihren geschäftlichen Abläufen kombinieren, sodass Sie Ihre E-Commerce-Website nach den Anforderungen Ihres Unternehmens verwalten können.

Weitere Informationen über den Bitnami Magento-Stack.

Projektmanagementanwendungen

Lightsail hat derzeit ein Projektmanagement-Anwendungsimage, Redmine. Dieses Image verwendet Linux/Unix (Ubuntu) als Basis-Betriebssystem.

Redmine verpackt von Bitnami

Bitnami Redmine ist ein vorkonfiguriertes ready-to-use Image für den Betrieb von Redmine auf Lightsail. Redmine ist eine flexible Projektmanagement-Webanwendung. Sie bietet Unterstützung für mehrere Projekte, rollenbasierte Zugriffskontrolle, Gantt-Diagramme und Kalender, Verwaltung von Nachrichten, Dokumenten und Dateien, projektabhängige Wikis und Foren, SCM-Integration und vieles mehr.

Dieser Blueprint ist mit einem Lightsail-Instanzplan nur für IPv6 kompatibel.

Weitere Informationen über den Bitnami Redmine-Stack.

IPv6-onlyInstance-Pläne in Lightsail

Öffentliche, erreichbare IPv4-Adressen werden aufgrund ihrer weit verbreiteten Nutzung und ständig steigender globaler Nachfrage nur kurz angeboten. Der letzte verfügbare Block neuer IP-Adressen der Version 4 (IPv4) wurde 2011 zugewiesen. Seit dieser Zeit hat jeder einen endlichen Satz verfügbarer Adressen wiederverwendet. IP Version 6 (IPv6) ist der IP-Adressstandard der nächsten Generation. IPv6 ergänzt IPv4 und wird es schließlich ersetzen, um den Mangel an IP-Adressen zu beheben.

Was sind IPv6-onlyPläne?

Lightsail-Instance-Pläne bündeln ein Betriebssystem (OS) und eine Anwendung Ihrer Wahl. Sie unterstützen auch sowohl IPv4- als auch IPv6-Netzwerke (Dual-Stack) oder IPv6-onlyNetzwerke. Ein Dual-Stack-Plan weist Ihrer Instance eine öffentliche IPv4- und eine öffentliche IPv6-Adresse zu. Mit diesem Plan können Sie IPv6 nach Bedarf aktivieren oder deaktivieren. Bei einem IPv6-onlyInstance-Plan erhält Ihre Instance eine öffentliche IPv6-Adresse und unterstützt keinen öffentlichen IPv4-Datenverkehr. Informationen dazu, welche Lightsail-Plattformen und -Vorlagen IPv6-onlyPläne unterstützen, finden Sie unter Wählen Sie ein Amazon Lightsail-Instance-Image.

Erstellen Sie eine IPv6-onlyInstance, wenn Sie keine öffentliche IPv4-Adresse benötigen. Bevor Sie eine IPv6-onlyInstance erstellen, stellen Sie sicher, dass Sie über IPv6 kommunizieren können. Weitere Informationen finden Sie unter IPv6-Erreichbarkeit in Überprüfen der IPv6-Erreichbarkeit in Lightsail. Informationen zum Migrieren einer vorhandenen Instance von Dual-Stack zu IPv6-only oder von IPv6-only zu Dual-Stack finden Sie unter Erstellen einer Lightsail-Instance aus einem Snapshot.

Überlegungen zu IPv6

Lesen Sie die folgenden Überlegungen, bevor Sie eine IPv6-onlyInstance erstellen:

- Stellen Sie sicher, dass Ihre Netzwerkinfrastruktur und Ihr Internetdienstanbieter (ISP) beide IPv6-compatible sind. Weitere Informationen finden Sie unter Überprüfen der IPv6-Erreichbarkeit in Lightsail.
- Stellen Sie sicher, dass Ihre Anwendung und Benutzer über IPv6 kommunizieren können. Weitere Informationen finden Sie unter Überprüfen der IPv6-Erreichbarkeit in Lightsail.

- Ihre Instance kommuniziert nur öffentlich über IPv6. Es erhält auch eine private IPv4-Adresse für die Kommunikation mit anderen Ressourcen in Ihrem Lightsail-Konto. IPv6-onlyInstances unterstützen keinen ein- oder ausgehenden öffentlichen IPv4-Datenverkehr. Weitere Informationen finden Sie unter IP-Adressen in Amazon Lightsail.
- Die browserbasierten Lightsail-SSH- und RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um SSH oder RDP über IPv6 in Ihre Instance zu übertragen. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.
- IPv6-onlyInstances können derzeit nicht als Ursprung für eine Lightsail Content Delivery Network (CDN)-Verteilung konfiguriert werden.

Migrieren zu einer IPv6-onlyInstance

Sie können eine vorhandene Dual-Stack-Instance zu einem IPv6-onlyPlan migrieren. Bevor Sie beginnen, empfehlen wir Ihnen, den vorherigen Überlegungen zu IPv6 Abschnitt zu lesen.

Erstellen Sie zur Migration einen Snapshot Ihrer Dual-Stack-Instance und anschließend eine neue Instance aus dem Snapshot. Wählen Sie während des Workflows zum Erstellen einer Instance den IPv6-onlyNetzwerkplan aus. Ausführliche Informationen zu diesem Verfahren finden Sie unter Erstellen einer Lightsail-Instance aus einem Snapshot.

Um von einem IPv6-onlyInstance-Plan zu einem Dual-Stack-Plan zu migrieren, wählen Sie stattdessen den Dual-Stack-Plan aus.

SSH-Schlüsselpaare in Lightsail

Ein Schlüsselpaar ist ein Satz von Sicherheitsanmeldeinformationen, mit denen Sie Ihre Identität nachweisen, wenn Sie eine Verbindung zu einer Amazon Lightsail-Instance herstellen. Ein Schlüsselpaar besteht aus einem privaten und einem öffentlichen Schlüssel. Lightsail speichert den öffentlichen Schlüssel auf Ihrer Instance, und Sie speichern den privaten Schlüssel.

Die Schlüsselpaar-Dateien enthalten den folgenden Text:

Unter Linux- und Unix-Instances können Sie mit dem privaten Schlüssel eine sichere SSH-Verbindung zu Ihrer Instance herstellen. Bei Windows-Instances entschlüsselt der private Schlüssel das Standard-Administratorkennwort, das Sie zum Herstellen einer sicheren RDP-Verbindung zu Ihrer Instance verwenden.

Jeder, der Zugriff auf Ihren privaten Schlüssel hat, kann sich mit Ihren Instances verbinden. Daher ist es wichtig, dass Sie Ihren privaten Schlüssel an einem sicheren Ort aufbewahren.

Inhalt

Auswählen einer Schlüsselpaar-Option

Sie können beim Erstellen einer Lightsail-Instance eine der folgenden Schlüsselpaaroptionen auswählen. Windows-Instances verwenden immer den Standardschlüssel. Daher können Sie beim Erstellen von Windows-Instances kein Schlüsselpaar erstellen oder einen Schlüssel hochladen.

- Standardschlüsselpaar – Lightsail erstellt automatisch ein Standardschlüsselpaar in jedem , in AWS-Region dem Sie Instances erstellen. Wenn Sie das Standardschlüsselpaar mit Ihrer Instance verwenden, speichert Lightsail den öffentlichen Schlüssel auf Ihrer Instance. Sie können den privaten Schlüssel eines Standard-Schlüsselpaars jederzeit von der Seite Konto in der Lightsail-Konsole herunterladen. Sie können bis zu einem Standard-Schlüsselpaar in jedem AWS-Region haben.

- Schlüsselpaar erstellen (Linux- und Unix-Instances) – Sie können die Lightsail-Konsole verwenden, um ein neues benutzerdefiniertes Schlüsselpaar zur Verwendung mit Ihrer Instance zu erstellen. Wenn Sie ein benutzerdefiniertes Schlüsselpaar erstellen, geben Sie ihm einen eindeutigen Namen, und Lightsail speichert den öffentlichen Schlüssel auf Ihrer Instance. Sie können den privaten Schlüssel eines benutzerdefinierten Schlüsselpaares nur herunterladen, wenn Sie ihn zum ersten Mal erstellen.
- Schlüssel hochladen (Linux- und Unix-Instances) – Um ein vorhandenes Schlüsselpaar Ihres eigenen zu verwenden, können Sie Ihren öffentlichen Schlüssel in Lightsail hochladen. Wenn Sie einen öffentlichen Schlüssel zur Verwendung mit Ihrer Instance hochladen, geben Sie ihr einen eindeutigen Namen und Lightsail speichert ihn auf Ihrer Instance. Sie behalten und speichern den privaten Schlüssel Ihres Schlüsselpaares.

Wenn Sie einen einzelnen öffentlichen Schlüssel für mehrere Instances konfigurieren, können Sie denselben privaten Schlüssel des Schlüsselpaares verwenden, um eine Verbindung zu diesen Instances herzustellen. Weitere Informationen zum Verwalten von Schlüsselpaaren finden Sie unter Verwalten von Schlüsselpaaren in Amazon Lightsail.

Eine Verbindung mit Ihren Instances herstellen

Sie können sich mit einer der folgenden Optionen mit Ihren Lightsail-Instances verbinden.

Browserbasierte Lightsail-SSH- und RDP-Clients

In der Lightsail-Konsole können Sie über einen browserbasierten SSH-Client sofort eine Verbindung zu Ihren Linux- und Unix-Instances herstellen und über einen browserbasierten RDP-Client eine Verbindung zu Ihren Windows-Instances herstellen. Die browserbasierten Lightsail-SSH- und RDP-Clients akzeptieren nur IPv4-Datenverkehr. Erstellen Sie eine Dual-Stack-Instance oder verwenden Sie einen Drittanbieter-Client, um über IPv6 SSH oder RDP in Ihre Instance zu senden. Sie müssen keinen SSH-Client auf Ihrem Computer installieren, Schlüsselpaare konfigurieren oder Administratorkennwörter angeben, wenn Sie über die browserbasierten Clients eine Verbindung zu Ihren Instances herstellen. Dies ist der schnellste Weg, um eine Verbindung zu Ihren Instances herzustellen. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Linux- oder Unix-Instance in Amazon Lightsail und unter Herstellen einer Verbindung mit Ihrer Windows-Instance in Amazon Lightsail.

Die browserbasierten Clients verwenden ein anderes Schlüsselpaar als das, das Sie beim Erstellen Ihrer Instances konfigurieren, z. B. den Standardschlüssel oder einen Schlüssel, den Sie erstellen

oder hochladen. Selbst wenn Sie einen der ursprünglich konfigurierten Schlüssel löschen oder verlieren, können Sie sich weiterhin über die browserbasierten Clients mit Ihren Instances verbinden.

SSH- und RDP-Clients Dritter

Sie können sich über einen SSH-Client eines Drittanbieters mit Ihren Linux- und Unix-Instances verbinden und sich über einen RDP-Client eines Drittanbieters mit Ihren Windows-Instances verbinden. Wenn Sie einen SSH-Client verwenden, müssen Sie ihn so konfigurieren, dass er den privaten Schlüssel des Schlüsselpaares verwendet, das Sie auf Ihrer Instance konfiguriert haben. Wenn Sie einen RDP-Client verwenden, müssen Sie das Administratorkennwort Ihrer Windows-Instance angeben.

Wenn Sie einen Windows-Computer lokal verwenden, können Sie die folgenden Clients verwenden, um eine Verbindung zu Ihren Lightsail-Instances herzustellen.

- PuTTY – Verwenden Sie PuTTY, um über SSH eine Verbindung zu Linux- oder Unix-Instances herzustellen. Weitere Informationen finden Sie unter Einrichten von PuTTY, um eine Verbindung zu Ihrer Instance herzustellen.
- Remotedesktopverbindung – Verwenden Sie den Remotedesktopverbindungs-Client, um über RDP eine Verbindung zu Windows-Instances herzustellen. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Ihrer Windows-Instance mithilfe des Remote-Desktop-Verbindungs-Clients auf einem Windows-Computer.

Wenn Sie einen Mac-Computer lokal verwenden, verwenden Sie die folgenden Clients, um eine Verbindung zu Ihren Lightsail-Instances herzustellen.

- Nativer SSH-Client in Terminal – Verwenden Sie den nativen SSH-Client in Terminal, um eine Verbindung mit Linux- und Unix-Instances herzustellen. Weitere Informationen finden Sie unter Herstellung einer Verbindung zu Ihrer Linux- oder Unix-Instance mit SSH in Terminal.
- Microsoft Remote Desktop – Verwenden Sie den Microsoft-Remote-Desktop-Client für macOS, um über RDP eine Verbindung zu Windows-Instances herzustellen. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Ihrer Windows-Instance mithilfe des Microsoft-Remote-Desktop-Clients auf einem Mac.

Verwalten von in Instances gespeicherten Schlüsseln

Nachdem Ihre Instance ausgeführt wurde, können Sie der Instance einen neuen Schlüssel hinzufügen oder den Schlüssel ersetzen, den Sie ihr ursprünglich zugewiesen haben. Beispiel:

Falls ein Benutzer in Ihrer Organisation mithilfe eines separaten Schlüssels Zugriff auf das Systembenutzerkonto benötigt, können Sie diesen Schlüssel zu Ihrer Instance hinzufügen. Ein anderes Beispiel könnte sein, wenn jemand Ihre Organisation verlässt und eine Kopie der Datei des privaten Schlüssels (.PEM) hat. Sie können verhindern, dass sie sich mit Ihrer Instance verbinden, indem Sie den Schlüssel durch einen neuen ersetzen oder vollständig entfernen. Weitere Informationen finden Sie unter Verwalten von Schlüsseln, die auf einer Instance in Amazon Lightsail gespeichert sind.

Themen

- Herstellen einer Verbindung zu Ihren Lightsail-Linux- oder Unix-Instances
- Herstellen einer Verbindung mit Ihrer Lightsail-Windows-Instance

Herstellen einer Verbindung zu Ihren Lightsail-Linux- oder Unix-Instances

Amazon Lightsail bietet Ihnen einen browserbasierten SSH-Client, der die schnellste Möglichkeit darstellt, eine Verbindung zu Ihrer Linux- oder Unix-Instance herzustellen. Für die Verbindung zu Ihrer Instance können Sie auch Ihren eigenen SSH-Client nutzen. Weitere Informationen finden Sie unter PuTTY herunterladen und einrichten.

Verbinden Sie sich mit Ihrer Instance mit SSH, um administrative Aufgaben auf dem Server auszuführen, wie z. B. die Installation von Software-Paketen oder die Konfiguration von Webanwendungen. Der browserbasierte SSH-Client benötigt keine Softwareinstallation und ist fast unmittelbar nach dem Erstellen einer Instance verfügbar.

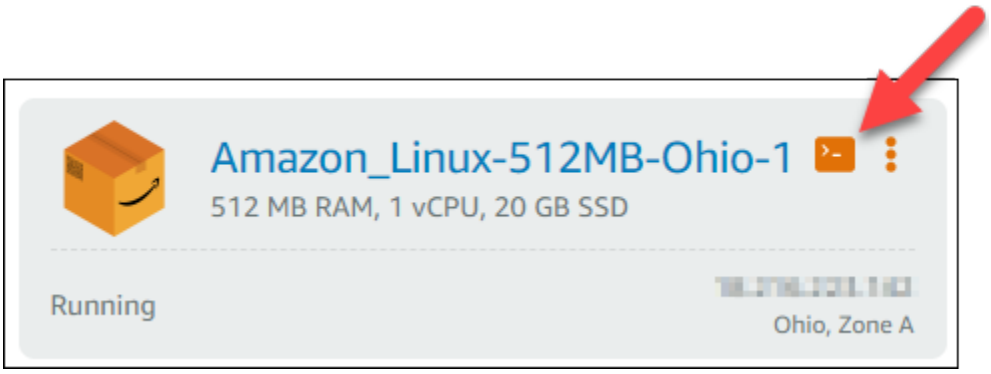
> **Note**
>
> Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um SSH oder RDP über IPv6 in Ihre Instance zu übertragen. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.
>
> Informationen zum Herstellen einer Verbindung mit einer Windows Server-Instance in Lightsail finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-basierten Instance.

So verbinden Sie sich mit Ihrer Linux- oder Unix-Instance

1. Melden Sie sich bei der Lightsail-Konsole an.

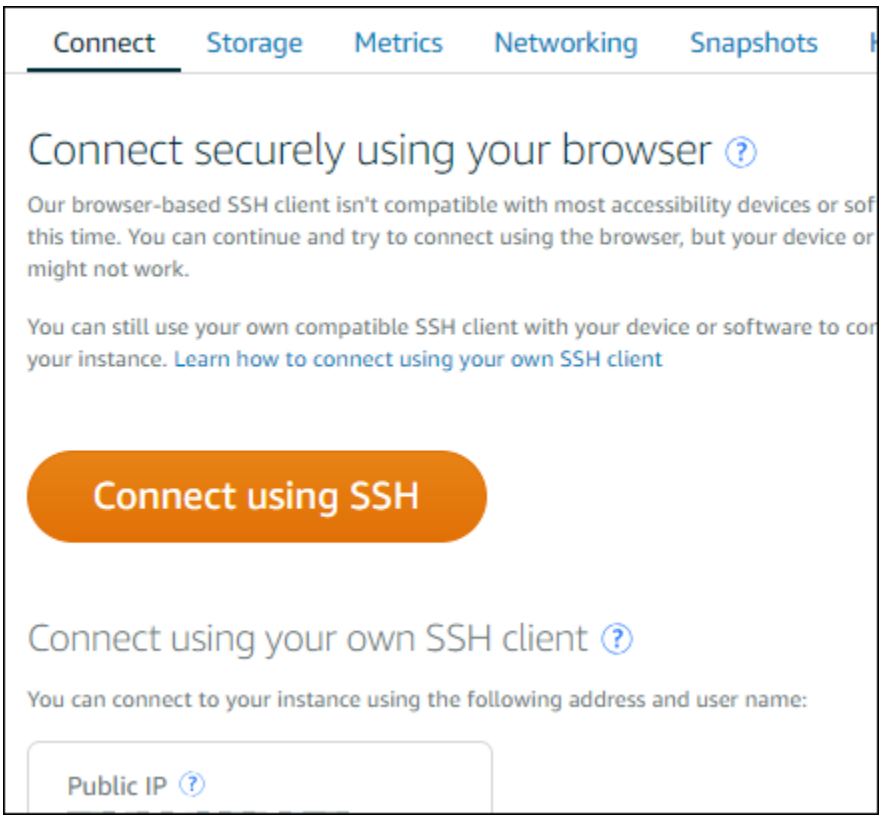
2. Rufen Sie den browserbasierten SSH-Client für die Instance, mit der Sie sich verbinden möchten, mit einer der folgenden Methoden auf:

   - Wählen Sie das Schnellverbindungssymbol, wie im folgenden Beispiel gezeigt.

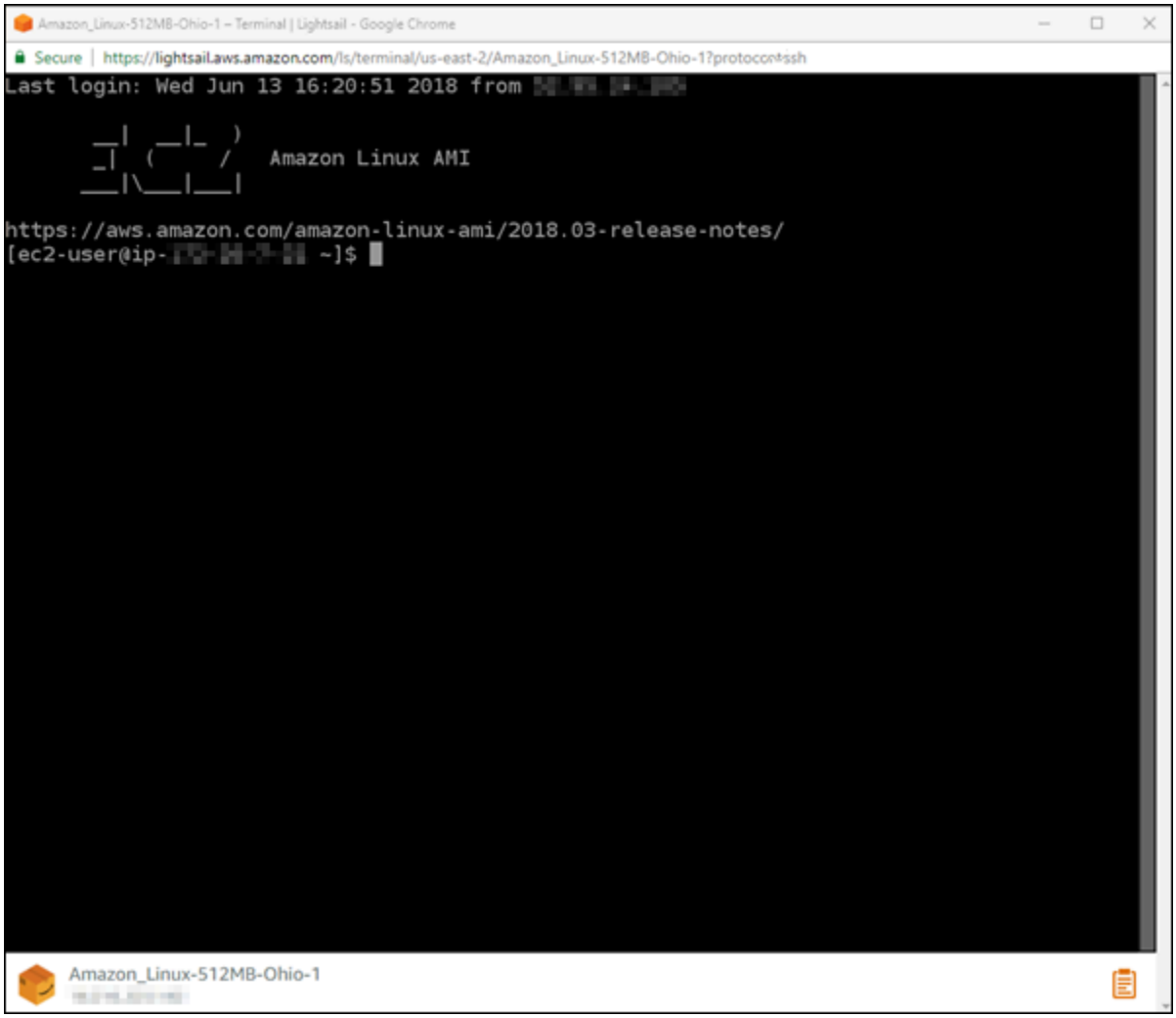


   - Klicken Sie auf das Aktionsmenüsymbol (⋮) und wählen Sie dann Connect (Verbinden).

   - Wählen Sie den Namen der Instance und wählen Sie dann auf der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).



Sie können die Interaktion mit Ihrer Instance beginnen, wenn sich der browserbasierte SSH-Client öffnet und ein Terminal-Fenster angezeigt wird, wie im folgenden Beispiel gezeigt:



> **Note**
>
> Die Registerkarte Connect (Verbinden) stellt auch die erforderlichen Informationen bereit, um eine Verbindung mit Ihrem eigenen SSH-Client herzustellen. Weitere Informationen finden Sie unter PuTTY herunterladen und einrichten.

Interagieren Sie mit Ihrer Linux- oder Unix-Instance über den browserbasierten SSH-Client.

Geben Sie Linux- oder Unix-Befehle direkt in das Terminalfenster ein, fügen Sie Text in den Terminalfenster ein oder kopieren Sie Text aus dem Terminalfenster des browserbasierten SSH-Clients. In den folgenden Abschnitten erfahren Sie, wie Sie in SSH Text in die Zwischenablage kopieren und aus der Zwischenablage einfügen.

So fügen Sie Text in den browserbasierten SSH-Client ein

1. Markieren Sie Text in Ihrem lokalen Desktop, drücken Sie dann Ctrl+C (STRG+C) oder Cmd+C, um ihn in Ihre lokale Zwischenablage zu kopieren.
2. Wählen Sie in der rechten unteren Ecke des browserbasierten SSH-Clients das Zwischenablagesymbol. Das Textfeld der browserbasierten SSH-Client-Zwischenablage wird angezeigt.
3. Klicken Sie in das Textfeld und drücken Sie dann Ctrl+V (STRG+V) oder Cmd+V,, um den Inhalt aus Ihrer lokalen Zwischenablage in die browserbasierte SSH-Client-Zwischenablage einzufügen.
4. Klicken Sie mit der rechten Maustaste auf einen beliebigen Bereich auf dem SSH-Terminalfenster, um den Text aus der Zwischenablage des browserbasierten SSH-Client auf dem Terminalbildschirm einzufügen.

So kopieren Sie Text vom browserbasierten SSH-Client

1. Markieren Sie Text auf dem Terminalbildschirm.

2. Wählen Sie in der rechten unteren Ecke des browserbasierten SSH-Clients das Zwischenablagesymbol. Das Textfeld der browserbasierten SSH-Client-Zwischenablage wird angezeigt.
3. Markieren Sie den Text, den Sie kopieren möchten, drücken Sie dann Ctrl+C (STRG+C) oder Cmd+C, um den Text in Ihre lokale Zwischenablage zu kopieren. Sie können den kopierten Text nun an beliebiger Stelle auf Ihrem lokalen Desktop einfügen.

Einrichten eines SSH-Schlüssel für Lightsail

Secure SHell (SSH) ist ein Protokoll für eine sichere Verbindung zu einem Virtual Private Server (oder einer Lightsail-Instance). SSH erzeugt einen öffentlichen Schlüssel und einen privaten Schlüssel, die den externen Server mit einem autorisierten Benutzer gleichsetzen. Unter Verwendung dieses Schlüsselpaars können Sie unter Verwendung eines Browser-basierten SSH-Terminals eine Verbindung zu Ihrer Lightsail-Instance einrichten.

Weitere Informationen zu SSH finden Sie unter SSH verstehen.

Wenn Sie Ihre Lightsail-Instance einrichten, ist die Standardoption, die Verwaltung Ihrer SSH-Schlüssel Lightsail zu überlassen. Lightsail bietet einen Browser-basierten SSH-Client für eine

sichere Verbindung zu Ihrer Linux-basierten Instance. Es handelt sich um ein voll funktionsfähiges Terminal, auf dem Sie Befehle eingeben und Änderungen an der Instance vornehmen können.

Windows-basierte Instances verwenden das RDP-Protokoll (Remote Desktop Protocol) anstelle von SSH. Weitere Informationen zu Windows-basierten Instances in Lightsail finden Sie unter Erste Schritte mit Windows-basierten Instances in Lightsail.

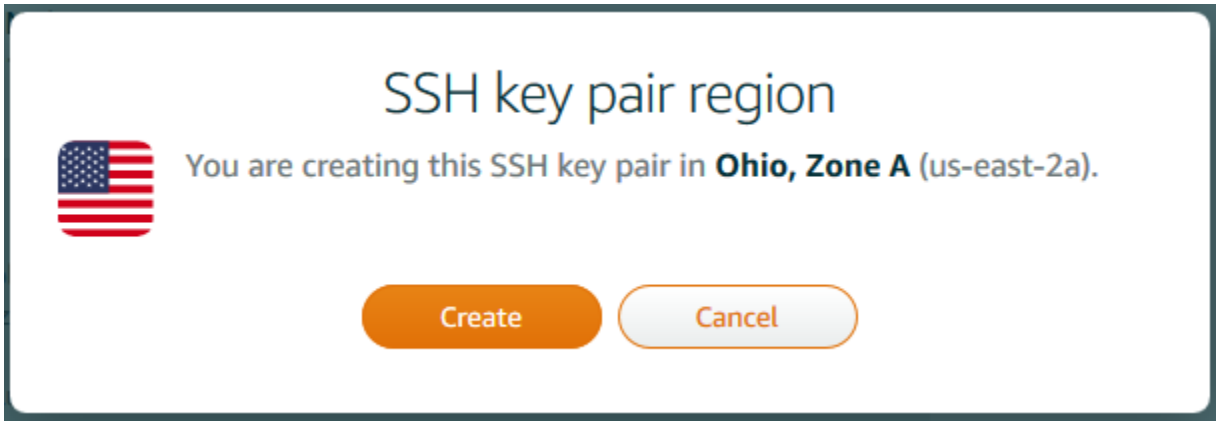
> **Important**
>
> Das SSH-Schlüssel-Management ist regional. Wenn Sie eine Instance in einer neuen AWS-Region erstellen, haben Sie die Möglichkeit, das Standard-Schlüsselpaar für die betreffende Region zu verwenden. Sie können auch einen benutzerdefinierten Schlüssel in dieser Region verwenden. Wenn Sie einen eigenen Schlüssel hochladen, müssen Sie dies für jede Region machen, in der Sie eine Lightsail-Instance haben.

Wenn Sie den Standardschlüssel verwenden, können Sie trotzdem den privaten Schlüssel für die Aufbewahrung herunterladen. Dies kann entweder zum Zeitpunkt der Erstellung der Instance oder später erfolgen. Wenn Sie entscheiden, den Schlüssel herunterzuladen, nachdem Sie Ihre Instance erstellt haben, können Sie dies unter SSH keys (SSH-Schlüssel) auf der Account (Konto)-Seite erledigen.

Erstellen eines neuen Schlüssels

Wenn Sie festlegen, nicht den Standardschlüssel zu verwenden, können Sie ein neues Schlüsselpaar erstellen, wenn Sie Ihre Lightsail-Instance erstellen.

1. Falls dies noch nicht geschehen ist, wählen Sie Create instance (Instance erstellen).
2. Wählen Sie auf der Seite Create an instance (Eine Instance erstellen) die Option Change SSH key pair (SSH-Schlüsselpaar wechseln).
3. Wählen Sie Neu erstellen.
4. Lightsail zeigt die Region an, für die wir den neuen Schlüssel erstellen.



Wählen Sie Erstellen aus.

5. Geben Sie einen Namen für Ihr Schlüsselpaar ein.

   Ressourcennamen:

   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

6. Wählen Sie Schlüsselpaar generieren.

   > ⚠ Important
   >
   > Speichern Sie Ihren Schlüssel an einem Ort, wo Sie ihn gut wiederfinden können. Außerdem sollten Sie sicherstellen, dass die Berechtigungen so eingestellt sind, dass niemand anderer ihn lesen kann.

7. Fahren Sie mit der Erstellung der Instance fort.

Einen vorhandenen Schlüssel hochladen

Sie können außerdem festlegen, einen vorhandenen Schlüssel hochzuladen, wenn Sie Ihre Lightsail-Instance erstellen.

1. Falls dies noch nicht geschehen ist, wählen Sie Create instance (Instance erstellen).
2. Wählen Sie auf der Seite Create an instance (Eine Instance erstellen) die Option Change SSH key pair (SSH-Schlüsselpaar wechseln).

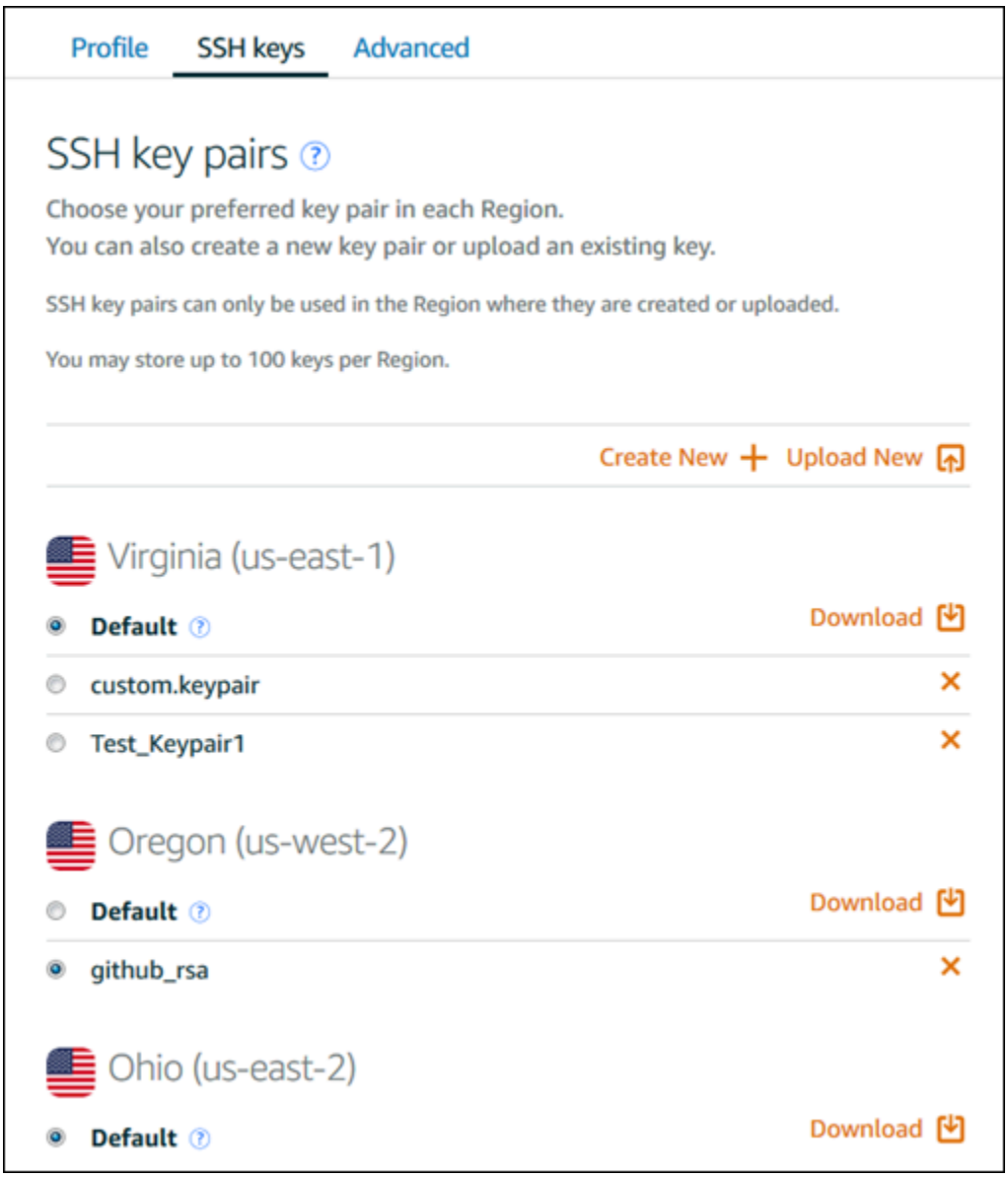
3. Klicken Sie auf Upload new (Jetzt hochladen).
4. Lightsail zeigt die Region an, für die wir den neuen Schlüssel hochladen.

   Klicken Sie auf Hochladen.
5. Klicken Sie auf Browse (Durchsuchen), um den Schlüssel auf Ihrem lokalen Computer zu suchen.

   Stellen Sie sicher, dass Sie einen öffentlichen Schlüssel hochladen (keinen privaten Schlüssel). Zum Beispiel `github_rsa.pub`.
6. Klicken Sie auf Upload key (Schlüssel hochladen).
7. Fahren Sie mit der Erstellung der Instance fort.

Ihre Schlüssel verwalten

Sie können Ihre Schlüssel auf der Registerkarte SSH keys (SSH-Schlüssel) der Account (Konto)-Seite verwalten. Sie sehen die Schlüsselpaare, die in den verschiedenen Regionen verwendet werden.



Auf dieser Seite können Sie den Schlüssel ändern, der standardmäßig verwendet werden soll, wenn Sie einen neuen Lightsail-Instance erstellen. Sie können auch einen neuen Schlüssel erstellen oder einen privaten Schlüssel herunterladen. Sie können einen SSH-Client wie PuTTY für die Verbindung verwenden, wozu Sie die private Hälfte des Schlüssels besitzen müssen. Sie können den Schlüssel von der Account (Konto)-Seite herunterladen. Weitere Informationen zum Einrichten von PuTTY, um eine Verbindung mit einer Lightsail-Instance herzustellen.

Stellen Sie mit dem SSH-Befehl eine Connect zu Ihrer Linux/UNIX-basierten Lightsail-Instance her

Wenn Ihr lokaler Computer ein Linux- oder Unix-Betriebssystem, einschließlich macOS, verwendet, können Sie mithilfe des SSH-Clients über ein Terminalfenster eine Verbindung zu Ihrer Linux- oder Unix-Instance in Amazon Lightsail herstellen.

Die in diesem Leitfaden beschriebene Methode zum Herstellen einer Verbindung mit Ihrer Instance ist eine von vielen. Weitere Informationen zu anderen Methoden finden Sie unter SSH-Schlüsselpaare.

Der einfachste Weg, eine Verbindung zu Ihrer Linux- oder Unix-Instanz in Lightsail herzustellen, ist die Verwendung des browserbasierten SSH-Clients, der in der Lightsail-Konsole verfügbar ist. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Linux- oder Unix-Instance.

> **Important**
>
> Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Verkehr. Verwenden Sie einen Drittanbieter-Client für SSH- oder RDP-Verbindungen zu Ihrer Instance über IPv6. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

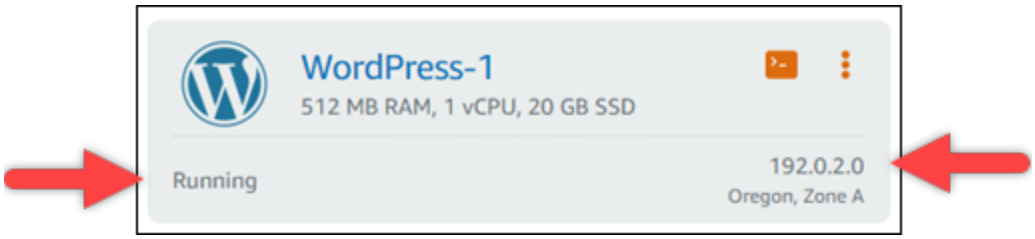
Inhalt

Schritt 1: Bestätigen Sie, dass Ihre Instance ausgeführt wird, und rufen Sie die öffentliche IP-Adresse ab

Im folgenden Verfahren melden Sie sich bei der Lightsail-Konsole an, um zu überprüfen, ob sich Ihre Instance im laufenden Zustand befindet, und um die öffentliche IP-Adresse Ihrer Instance abzurufen. Ihre Instance muss sich im laufenden Zustand befinden, um eine SSH-Verbindung herzustellen, und Sie benötigen die öffentliche IP-Adresse Ihrer Instance, um später in diesem Leitfaden eine Verbindung herzustellen.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Suchen Sie auf der Lightsail-Startseite auf der Registerkarte „Instanzen“ die Instanz, zu der Sie eine Verbindung herstellen möchten.
3. Bestätigen Sie, dass sich die Instance in einem ausgeführten Zustand befindet, und notieren Sie sich die öffentliche IP-Adresse Ihrer Instance.

   Der Status Ihrer Instance und ihre öffentliche IP-Adresse werden neben dem Namen Ihrer Instance aufgeführt, wie im folgenden Beispiel gezeigt.



Schritt 2: Bestätigen Sie das SSH-Schlüsselpaar, das von Ihrer Instance verwendet wird

Im folgenden Verfahren bestätigen Sie das SSH-Schlüsselpaar, das von Ihrer Instance verwendet wird. Sie benötigen den privaten Schlüssel des Schlüsselpaares, um sich bei Ihrer Instance zu authentifizieren und eine SSH-Verbindung herzustellen.

1. Wählen Sie auf der Lightsail-Startseite auf der Registerkarte Instanzen den Namen der Instanz aus, zu der Sie eine Verbindung herstellen möchten.

   Die Seite Verwaltung von Instances wird mit verschiedenen Registerkarten angezeigt, um Ihre Instance zu verwalten.

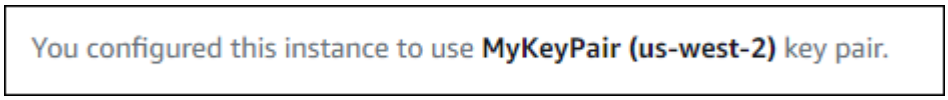
2. Scrollen Sie in der Registerkarte Verbinden nach unten, um das Schlüsselpaar anzuzeigen, das von Ihrer Instance verwendet wird. Zwei Möglichkeiten sind möglich:

   1. Das folgende Beispiel zeigt eine Instance, die das Standard-Schlüsselpaar für die AWS-Region verwendet, in der Sie Ihre Instance erstellt haben. Wenn Ihre Instance das Standardschlüsselpaar verwendet, können Sie mit Schritt 3 dieses Verfahrens fortfahren, um den privaten Schlüssel des Schlüsselpaars herunterzuladen. Lightsail speichert den privaten Schlüssel nur für das Standardschlüsselpaar jeder AWS-Region.

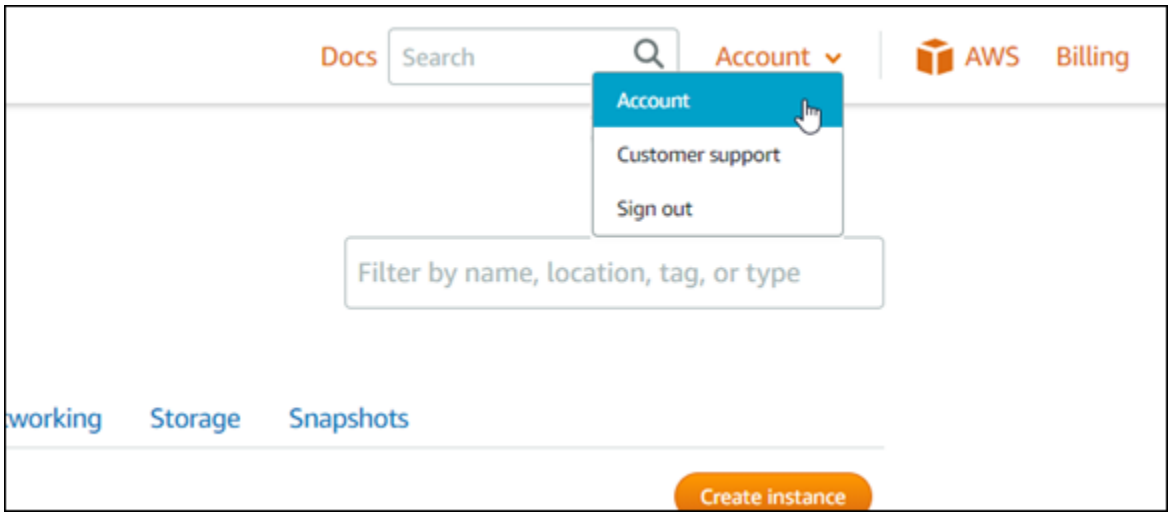
      > You configured this instance to use **default (us-west-2)** key pair.
      > You can download your default private key from the Account page.

   2. Das folgende Beispiel zeigt eine Instance, die ein benutzerdefiniertes Schlüsselpaar verwendet, das Sie entweder hochgeladen oder erstellt haben. Wenn Ihre Instance ein benutzerdefiniertes Schlüsselpaar verwendet, müssen Sie den privaten Schlüssel des benutzerdefinierten Schlüsselpaars suchen, in dem Sie Ihre Schlüssel speichern. Wenn Sie den privaten Schlüssel des benutzerdefinierten Schlüsselpaares verloren haben, können Sie keine SSH-Verbindung zu Ihrer Instance mit Ihrem eigenen Client herstellen. Sie können jedoch weiterhin den browserbasierten SSH-Client verwenden, der in der Lightsail-

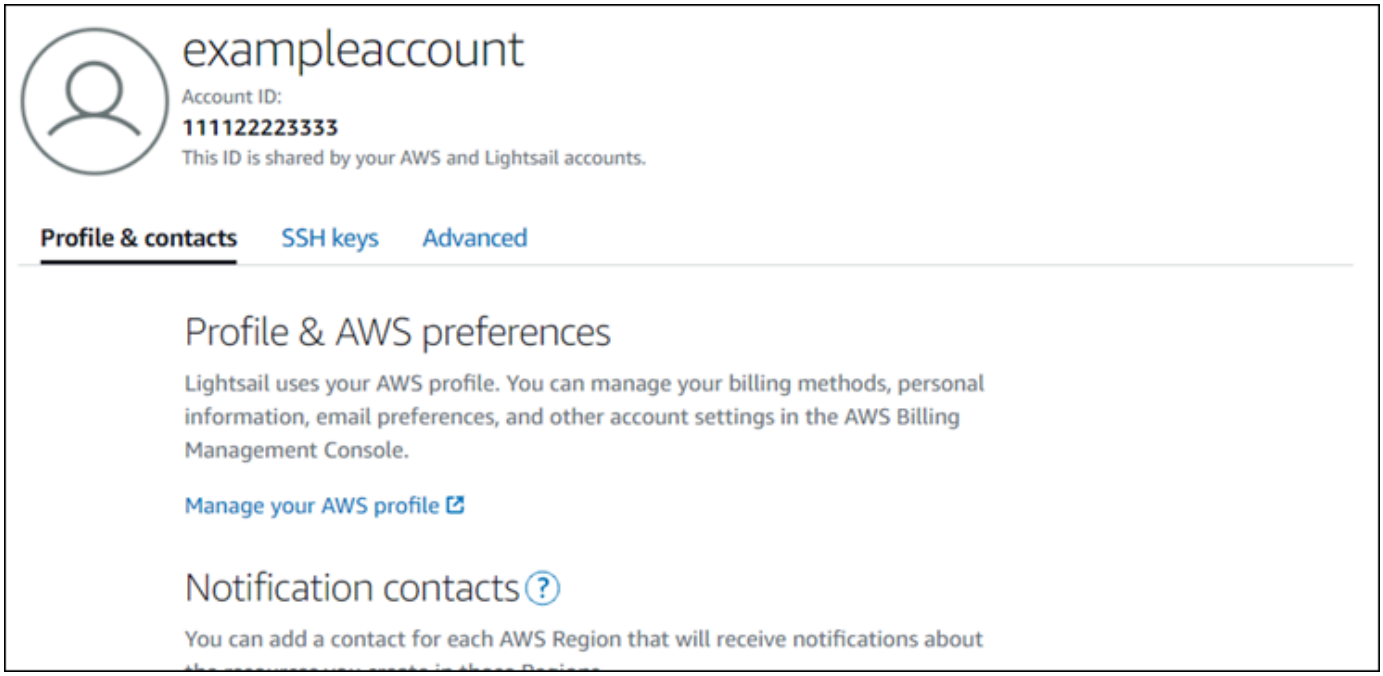
Konsole verfügbar ist. Fahren Sie fort mit dem nächsten Abschnitt Schritt 3: Ändern Sie die Berechtigungen Ihres privaten Schlüssels und stellen Sie eine Verbindung mit Ihrer Instance mithilfe von SSH her dieses Leitfadens, nachdem Sie den privaten Schlüssel des benutzerdefinierten Schlüsselpaares gefunden haben.



3. Wählen Sie in der Konto im oberen Navigationsmenü Account (Konto) aus.

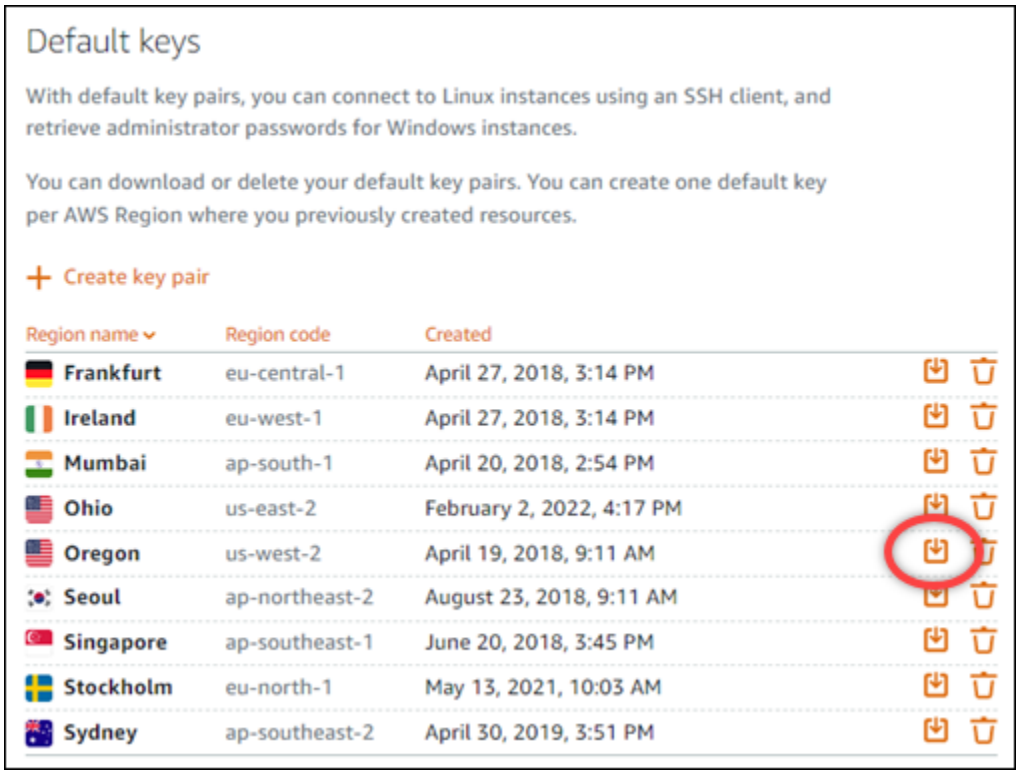


Die Seite Kontenverwaltung wird mit verschiedenen Registerkarten angezeigt, damit Sie Ihre Kontoeinstellungen verwalten können.



4. Wählen Sie die Registerkarte SSH-Schlüssel aus.

5. Scrollen Sie nach unten und wählen Sie das Download-Symbol neben dem Standardschlüssel der AWS-Region der Instance, mit der Sie eine Verbindung herstellen möchten.



Der private Schlüssel wird auf Ihren lokalen Computer heruntergeladen. Möglicherweise möchten Sie den heruntergeladenen Schlüssel in ein Verzeichnis verschieben, in dem Sie alle SSH-Schlüssel speichern, z. B. einen Ordner „Keys“ im Home-Verzeichnis Ihres Benutzers. Sie müssen im nächsten Abschnitt dieses Leitfadens auf das Verzeichnis verweisen, in dem der private Schlüssel gespeichert ist. Wenn der private Schlüssel versucht, als ein anderes Format als `.pem` zu speichern, sollten Sie das Format vor dem Speichern manuell in `.pem` ändern.

> **Note**
>
> Lightsail bietet keine Hilfsprogramme zum Bearbeiten von `.pem` Dateien oder anderen Zertifikatsformaten. Wenn Sie das Format Ihrer privaten Schlüsseldatei konvertieren müssen, sind kostenlose und Open-Source-Tools wie OpenSSL leicht verfügbar.

Fahren Sie fort mit dem nächsten Abschnitt Schritt 3: Ändern Sie die Berechtigungen Ihres privaten Schlüssels und stellen Sie eine Verbindung mit Ihrer Instance mithilfe von SSH her dieses Leitfadens, um den privaten Schlüssel zu verwenden, den Sie gerade heruntergeladen haben, und eine SSH-Verbindung zu Ihrer Instance herzustellen.

Schritt 3: Ändern Sie die Berechtigungen Ihres privaten Schlüssels und stellen Sie eine Verbindung mit Ihrer Instance mithilfe von SSH her

Im folgenden Verfahren werden Sie die Berechtigungen für Ihre private Schlüsseldatei so ändern, dass sie nur für Sie lesbar und beschreibbar ist. Anschließend öffnen Sie ein Terminalfenster auf Ihrem lokalen Computer und führen den SSH-Befehl aus, um eine Verbindung mit Ihrer Instanz in Lightsail herzustellen.

1. Öffnen Sie ein Terminalfenster auf Ihrem lokalen Computer.
2. Geben Sie den folgenden Befehl ein, um den privaten Schlüssel des Schlüsselpaares nur von Ihnen lesbar und beschreibbar zu machen. Dies ist eine bewährte Sicherheitsmethode, die von einigen Betriebssystemen erforderlich ist.

   ```
   sudo chmod 400 /path/to/private-key.pem
   ```

   Ersetzen Sie im Befehl *`/path/to/private-key.pem`* mit dem Verzeichnispfad, zu dem Sie den privaten Schlüssel des Schlüsselpaares gespeichert haben, das von Ihrer Instance verwendet wird.

   Beispiel:

   ```
   sudo chmod 400 /Users/user/Keys/LightsailDefaultKey-us-west-2.pem
   ```
3. Geben Sie den folgenden Befehl ein, um über SSH eine Verbindung zu Ihrer Instanz in Lightsail herzustellen:

   ```
   ssh -i /path/to/private-key.pem username@public-ip-address
   ```

   Ersetzen Sie im Befehl Folgendes:

   - *`/path/to/private-key.pem`* mit dem Verzeichnispfad, zu dem Sie den privaten Schlüssel des Schlüsselpaares gespeichert haben, das von Ihrer Instance verwendet wird.
   - *`username`* mit dem Benutzernamen Ihrer Instance. Je nach Vorlage, die von Ihrer Instance verwendet wird, können Sie einen der folgenden Benutzernamen angeben:
     - AlmaLinux OS 9-, Amazon Linux 2-, Amazon Linux 2023-, CentOS Stream 9-, FreeBSD- und openSUSE-Instances: `ec2-user`
     - CentOS 7-Instanzen: `centos`

- Debian-Instances: `admin`
- Ubuntu-Instances: `ubuntu`
- Bitnami-Instances: `bitnami`
- Plesk-Instances: `ubuntu`
- cPanel & WHM-Instances: `centos`

- *`public-ip-address`*Ersetzen Sie es durch die öffentliche IP-Adresse Ihrer Instance, die Sie weiter oben in diesem Handbuch in der Lightsail-Konsole notiert haben.

Beispiel mit absoluten Pfad:

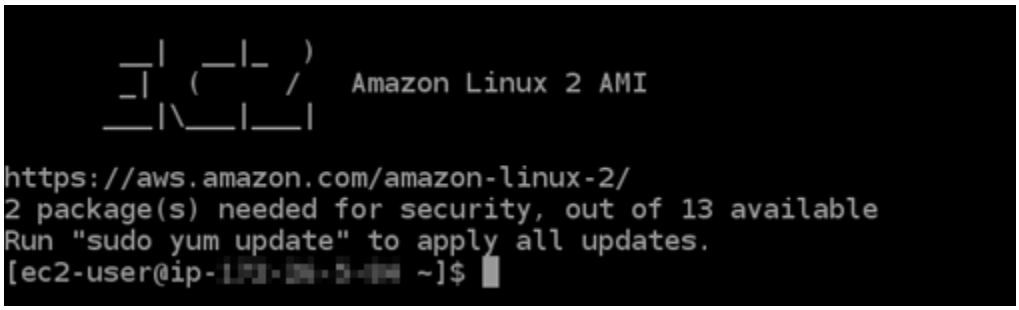
```
ssh -i /Users/user/Keys/LightsailDefaultKey-us-west-2.pem ec2-user@192.0.1.0
```

Beispiel mit relativem Pfad:

Beachten Sie, das `./` der `.pem`-Datei vorangestellt sein muss. Die Auslassung von `./` und das einfache Schreiben von `LightsailDefaultKey-us-west-2.pem` wird nicht funktionieren.

```
ssh -i ./LightsailDefaultKey-us-west-2.pem ec2-user@192.0.1.0
```

Sie sind erfolgreich mit Ihrer Instance verbunden, wenn die Willkommensnachricht für Ihre Instance angezeigt wird. Das folgende Beispiel zeigt die Willkommensnachricht für eine Amazon,Linux,2-Instance; andere Instance-Vorlagen haben eine ähnliche Willkommensnachricht. Nachdem Sie eine Verbindung hergestellt haben, können Sie Befehle auf Ihrer Instanz in Lightsail ausführen. Um die Verbindung zu trennen, geben Sie `exit` ein und drücken Sie auf Enter.



Herstellen einer Verbindung mit Ihrer Lightsail-Linux/Unix-basierten Instance mit PuTTY

Zusätzlich zum browserbasierten SSH-Terminal in Lightsail können Sie sich auch über einen SSH-Client wie PuTTY mit Ihrer Linux-basierten Instance verbinden. Informationen zum Einrichten von PuTTY finden Sie unter PuTTY herunterladen und einrichten, um eine Verbindung über SSH in Lightsail herzustellen.

> **Note**
>
> Informationen zum Herstellen einer Verbindung mit einer Windows-basierten Instance über RDP finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-basierten Lightsail-Instance.

Sie können den von Lightsail bereitgestellten privaten Standardschlüssel, einen neuen privaten Schlüssel von Lightsail oder einen anderen privaten Schlüssel verwenden, den Sie mit einem anderen -Service verwenden.

1. Starten Sie PuTTY (z. B. indem Sie im Start-Menü All Programs (Alle Programme), PuTTY, PuTTY wählen).
2. Wählen Sie Load (Laden) und suchen Sie dann Ihre gespeicherte Sitzung.

   Wenn Sie über keine gespeicherte Sitzung verfügen, lesen Sie nach unter Schritt 4: Beenden der Konfiguration von PuTTY mit Ihrem privaten Schlüssel und Instance-Informationen.
3. Melden Sie sich je nach Betriebssystem Ihrer Instance mit einem der folgenden Standardbenutzernamen an:

   - AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, FreeBSD und openSUSE-Instances: `ec2-user`
   - CentOS-7-Instances: `centos`
   - Debian-Instances: `admin`
   - Ubuntu-Instances: `ubuntu`
   - Bitnami-Instances: `bitnami`
   - Plesk-Instances: `ubuntu`
   - cPanel & WHM-Instances: `centos`

Weitere Informationen zu Instance-Betriebssystemen finden Sie unter Auswählen eines Images in Lightsail.

Weitere Informationen zu SSH finden Sie unter SSH und Herstellen einer Verbindung mit Ihrer Amazon Lightsail-Instance.

Herstellen einer Verbindung mit Ihrer Lightsail-Linux-Instance über SFTP

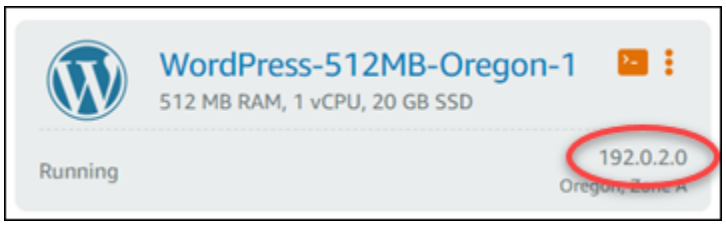
Sie können Dateien zwischen Ihrem lokalen Computer und Ihrer Linux- oder Unix-Instance in Amazon Lightsail übertragen, indem Sie über SFTP (SSH File Transfer Protocol) eine Verbindung zu Ihrer Instance herstellen. Zu diesem Zweck müssen Sie den privaten Schlüssel für Ihre Instance erhalten und dann dem FTP-Client konfigurieren. In diesem Tutorial erfahren Sie, wie Sie den FileZilla FTP-Client für die Verbindung mit Ihrer Instance konfigurieren. Diese Schritte kann sich auch für andere FTP-Clients.

Inhalt

Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies noch nicht geschehen ist:

- Laden Sie herunter und installieren Sie FileZilla auf Ihrem lokalen Computer. Weitere Informationen finden Sie unter den folgenden Downloadoptionen:
  - FileZilla Client für Windows herunterladen
  - FileZilla Client für Mac OS X herunterladen
  - FileZilla Client für Linux herunterladen
- Rufen Sie die öffentliche IP-Adresse Ihrer Instance ab. Melden Sie sich bei der Lightsail-Konsole an und kopieren Sie dann die öffentliche IP-Adresse, die neben Ihrer Instance angezeigt wird, wie im folgenden Beispiel gezeigt:

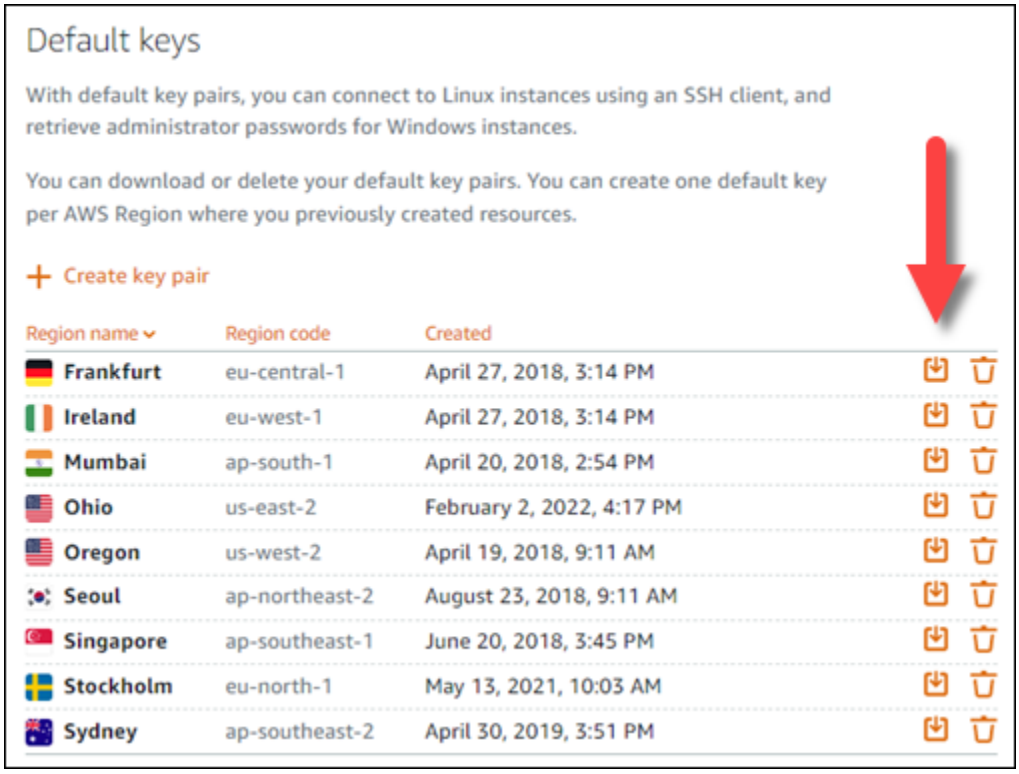


Abrufen des SSH-Schlüssels für Ihre Instance

Führen Sie die folgenden Schritte aus, um den privaten Standardschlüssel für die AWS-Region Ihrer Instance abzurufen, der für die Verbindung mit Ihrer Instance mithilfe von erforderlich ist FileZilla.

> **Note**
>
> Wenn Sie Ihr eigenes Schlüsselpaar verwenden oder ein Schlüsselpaar mit der Lightsail-Konsole erstellt haben, suchen Sie Ihren eigenen privaten Schlüssel und verwenden Sie ihn, um eine Verbindung zu Ihrer Instance herzustellen. Lightsail speichert Ihren privaten Schlüssel nicht, wenn Sie Ihren eigenen Schlüssel hochladen oder ein Schlüsselpaar mit der Lightsail-Konsole erstellen. Sie können keine Verbindung zu Ihrer Instance mit SFTP ohne Ihren privaten Schlüssel herstellen.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie in der oberen Navigationsleiste Account (Konto) und dann Account (Konto) aus der Dropdown-Liste.
3. Wählen Sie die Registerkarte SSH Keys (SSH-Schlüssel) aus.
4. Scrollen Sie nach unten bis zum Abschnitt Default keys (Standardschlüssel) auf der Seite.
5. Wählen Sie die Option Download neben dem standardmäßigen privaten Schlüssel für die Region, in der sich Ihre Instance befindet.

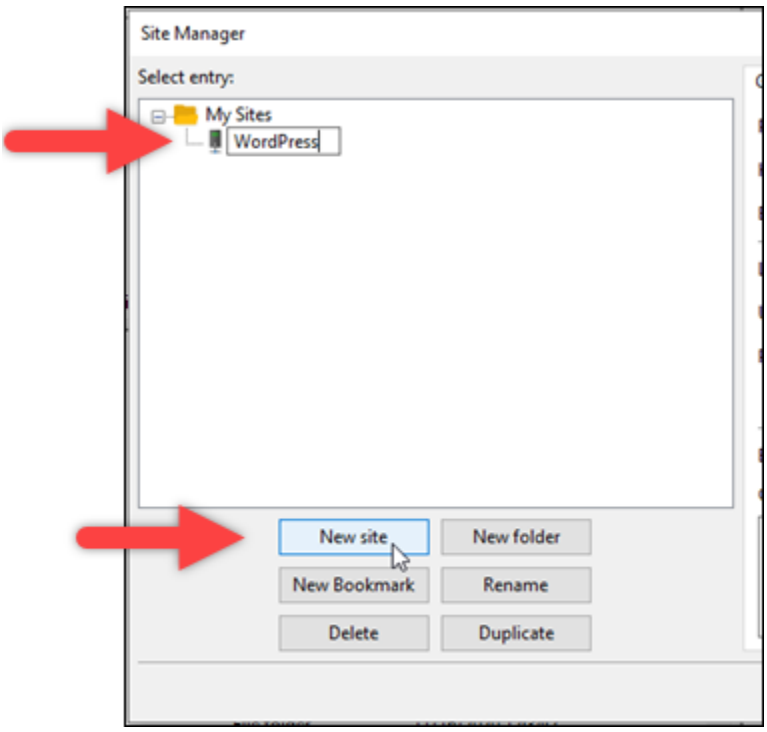


6. Speichern Sie Ihren privaten Schlüssel an einem sicheren Speicherort auf Ihrem lokalen Laufwerk.

Konfigurieren FileZilla und Herstellen einer Verbindung mit Ihrer Instance

Führen Sie die folgenden Schritte aus, um FileZilla für die Verbindung mit Ihrer Instance zu konfigurieren.

1. Öffnen Sie FileZilla.
2. Wählen Sie File (Datei), Site Manager.
3. Klicken Sie auf Neue Website und geben Sie Ihrer Website einen Namen.

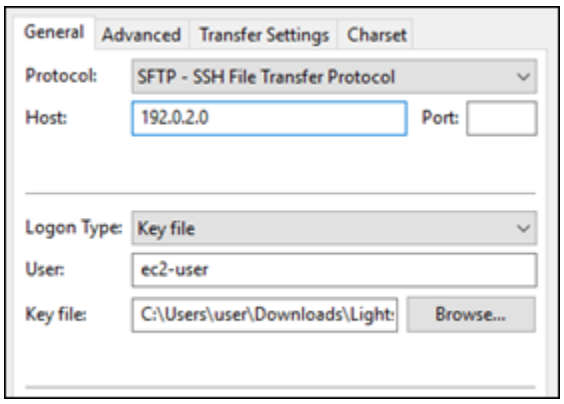


4. Wählen Sie im Dropdown-Menü Protocol (Protokoll) die Option SFTP – SSH File Transfer Protocol aus.
5. Geben Sie die öffentliche IP-Adresse Ihrer Instance in das Textfeld Host ein oder fügen Sie sie dort ein.
6. Wählen Sie im Dropdown-Menü Logon Type (Anmeldungstyp) die Option Key File (Schlüsseldatei) aus.
7. Geben Sie im Textfeld User (Benutzer) je nach dem Betriebssystem Ihrer Instance einen der folgenden Standardbenutzernamen ein

   - AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, FreeBSD und openSUSE-Instances: `ec2-user`
   - CentOS-7-Instances: `centos`
   - Debian-Instances: `admin`
   - Ubuntu-Instances: `ubuntu`
   - Bitnami-Instances: `bitnami`
   - Plesk-Instances: `ubuntu`
   - cPanel & WHM-Instances: `centos`

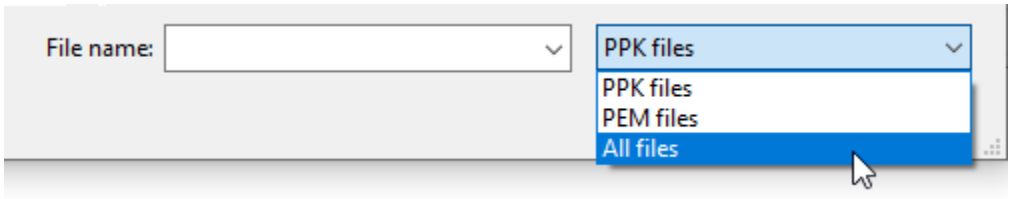
> **Important**
>
> Wenn Sie einen anderen Benutzernamen als die hier aufgeführten Standardbenutzernamen verwenden, müssen Sie dem Benutzer möglicherweise Schreibberechtigungen für Ihre Instance erteilen.

8. Wählen Sie neben dem Textfeld Key File (Schlüsseldatei) Browse (Durchsuchen).

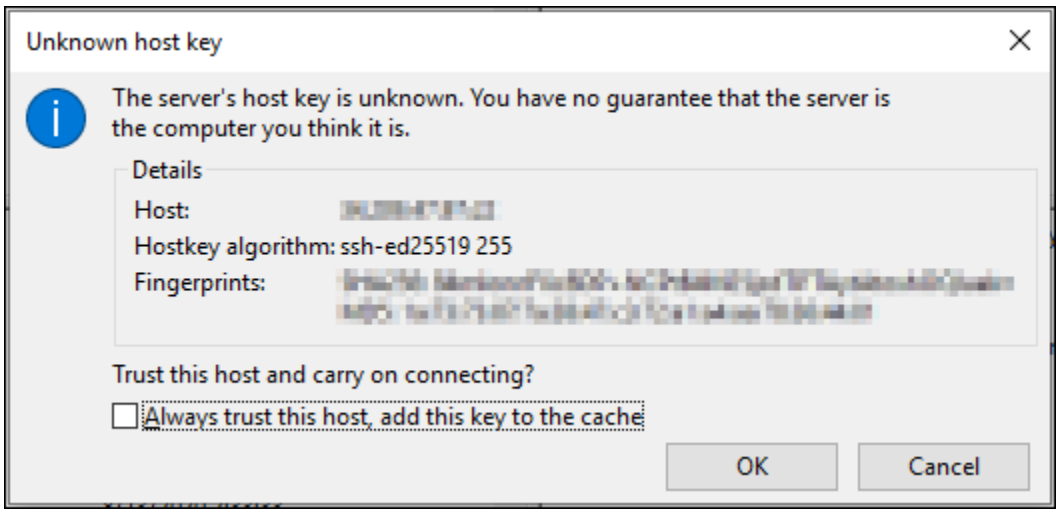


9. Suchen Sie die private Schlüsseldatei, die Sie zuvor in diesem Verfahren von der Lightsail-Konsole heruntergeladen haben, und wählen Sie dann Öffnen aus.

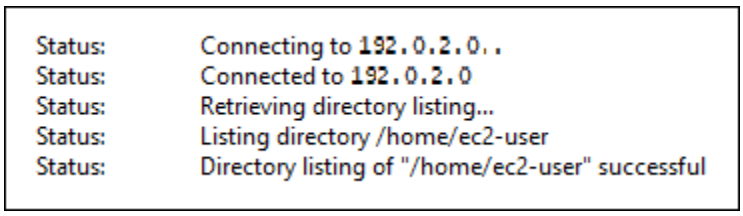
> **Note**
>
> Wenn Sie Windows verwenden, ändern Sie den Standarddateityp in Alle Dateien, wenn Sie nach Ihrer PEM-Datei suchen.



10. Wählen Sie Connect aus.
11. Möglicherweise wird eine Eingabeaufforderung angezeigt, ähnlich wie im folgenden Beispiel, dass der Hostschlüssel unbekannt ist. Klicken Sie auf OK, um die Eingabeaufforderung zu bestätigen und eine Verbindung mit Ihrer -Instance herzustellen.



Sie sind erfolgreich verbunden, wenn Sie Statusmeldungen ähnlich wie die im folgenden Beispiel sehen



Weitere Informationen zur Verwendung von FileZilla, einschließlich der Übertragung von Dateien zwischen Ihrem lokalen Computer und Ihrer Instance, finden Sie auf der FileZilla Wiki-Seite .

SSH-Schlüssel in Amazon Lightsail verwalten

Sie können mit Schlüsselpaaren eine sichere Verbindung zu Ihren Amazon Lightsail-Instances herstellen. Wenn Sie zum ersten Mal eine Amazon Lightsail-Instance erstellen, können Sie wählen, ob Sie ein Schlüsselpaar verwenden möchten, das Lightsail für Sie erstellt (das Lightsail-Standard-Schlüsselpaar) oder ein benutzerdefiniertes Schlüsselpaar, das Sie erstellen. Weitere Informationen finden Sie unter Schlüsselpaare und Herstellung einer Verbindung zu Instances in Amazon Lightsail.

Unter Linux- und Unix-Instances können Sie mit dem privaten Schlüssel eine sichere SSH-Verbindung zu Ihrer Instance herstellen. Bei Windows-Instances entschlüsselt der private Schlüssel das Standard-Administratorkennwort, das Sie zum Herstellen einer sicheren RDP-Verbindung zu Ihrer Instance verwenden.

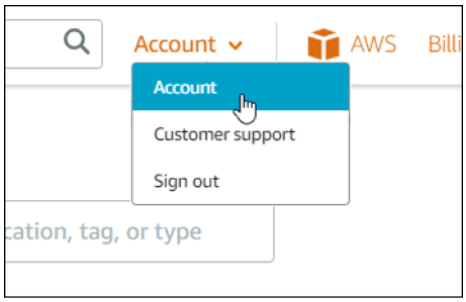
In diesem Leitfaden zeigen wir Ihnen, wie Sie die Schlüssel verwalten, die Sie mit Ihren Lightsail-Instances verwenden können. Sie können Ihre Schlüssel anzeigen, vorhandene Schlüssel löschen und neue Schlüssel erstellen oder hochladen.

Inhalt

Zeigen Sie Ihre Standard- und benutzerdefinierten Schlüssel

Führen Sie das folgende Verfahren aus, um Ihren Standard- und benutzerdefinierten Schlüssel über die Lightsail-Konsole anzuzeigen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite im oberen Navigationsmenü Account (Konto) aus.
3. Wählen Sie im Dropdown-Menü Konto aus.

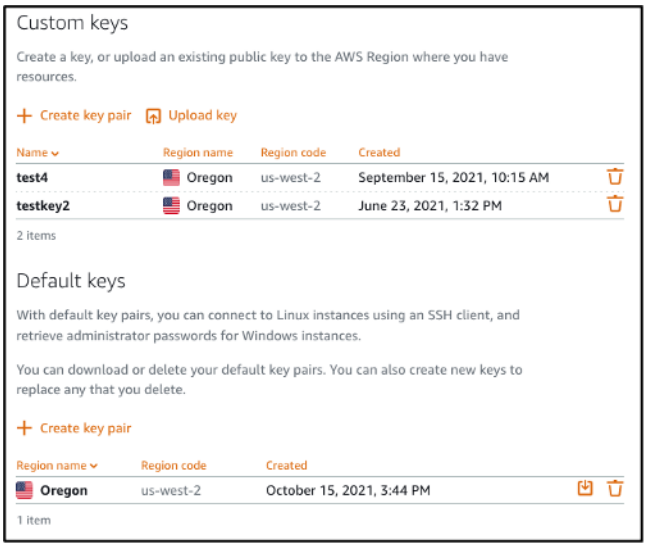


4. Wählen Sie die Registerkarte SSH-Schlüssel aus.

   Die SSH-Schlüssel-Seitenlisten:

   - Benutzerdefinierte Schlüssel – Dies sind Schlüssel, die Sie entweder mit der Lightsail-Konsole oder ein Tool eines Drittanbieters wie ssh-keygen erstellen. Sie können viele benutzerdefinierte Schlüssel in jedem AWS-Region haben.

- Standardschlüssel – Dies sind Schlüssel, die Lightsail für Sie erstellt. Sie können nur einen Standardschlüssel in jedem AWS-Region haben.



Benutzerdefinierte und Standardschlüssel sind regional. Zum Beispiel können Schlüssel in der AWS-Region USA West (Oregon) nur für Instances konfiguriert werden, die in dieser Region erstellt wurden. Weitere Informationen zu Schlüsseln finden Sie unter Schlüsselpaare und Herstellung einer Verbindung zu Instances in Amazon Lightsail.

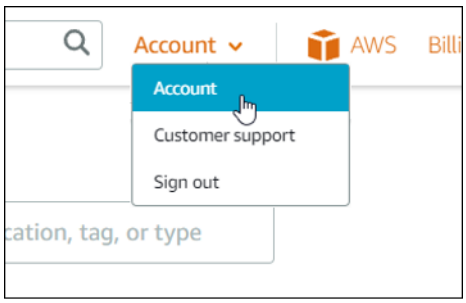
Auf der Seite SSH-Schlüssel können Sie Schlüsselpaare erstellen, Schlüssel hochladen, Schlüssel löschen und den privaten Schlüssel eines Lightsail-Standard-Schlüsselpaares herunterladen.

> **Note**
>
> Sie können den privaten Schlüssel eines benutzerdefinierten Schlüsselpaares nicht herunterladen, da Lightsail diesen Schlüssel nicht für Sie speichert. Wenn Sie den privaten Schlüssel eines benutzerdefinierten Schlüsselpaares verloren haben, sollten Sie einen neuen Schlüssel erstellen und ihn auf Ihrer Instance konfigurieren. Löschen Sie dann den Schlüssel, der verloren gegangen ist. Weitere Informationen finden Sie unter Erstellen eines benutzerdefinierten Schlüssels mit der Lightsail-Konsole oder Erstellen eines benutzerdefinierten Schlüssels mit ssh-keygen und ihn in Lightsail hochladen später in diesem Leitfaden.

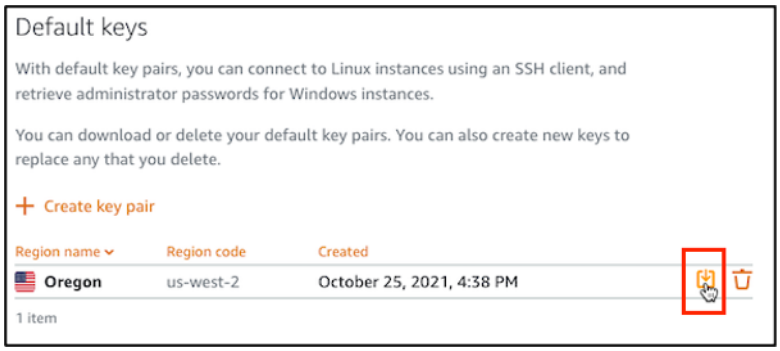
Laden Sie den privaten Schlüssel eines Standard-Schlüsselpaares aus der Lightsail-Konsole herunter

Führen Sie das folgende Verfahren aus, um den privaten Schlüssel eines Standardschlüsselpaares von der Lightsail-Konsole herunterzuladen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Homepage im oberen Navigationsbereich Account (Konto) aus.
3. Wählen Sie im Dropdown-Menü Konto aus.



4. Wählen Sie die Registerkarte SSH-Schlüssel aus.
5. Wählen Sie im Abschnitt Standardschlüssel der Seite das Download-Symbol für den Schlüssel, den Sie herunterladen möchten.



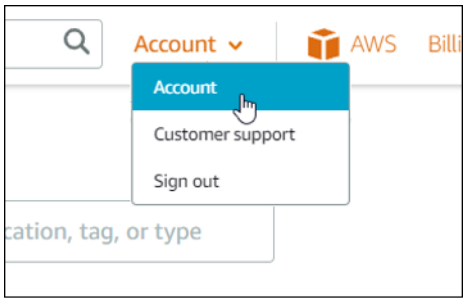
> **Important**
>
> Speichern Sie den privaten Schlüssel an einem sicheren Ort. Teilen Sie ihn nicht öffentlich, da er verwendet werden kann, um eine Verbindung zu Ihren Instances herzustellen.

Sie können einen SSH-Client für die Verbindung zu Ihren Instances mit dem privaten Schlüssel konfigurieren. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihren Instances.

Löschen eines benutzerdefinierten Schlüssels in der Lightsail-Konsole

Vervollständigen Sie den folgenden Vorgang, um einen benutzerdefinierten Schlüssel in der Lightsail-Konsole zu löschen. Dies verhindert, dass der benutzerdefinierte Schlüssel für neue Instances konfiguriert wird, die Sie in Lightsail erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Homepage im oberen Navigationsbereich Account (Konto) aus.
3. Wählen Sie im Dropdown-Menü Konto aus.



4. Wählen Sie die Registerkarte SSH-Schlüssel aus.
5. Wählen Sie im Abschnitt Benutzerdefinierte Schlüssel der Seite das Löschsymbol für den Schlüssel, den Sie löschen möchten.

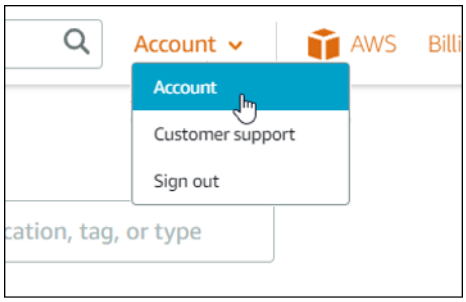
Dadurch wird der öffentliche Schlüssel des benutzerdefinierten Schlüsselpaares nicht aus Instances entfernt, die zuvor erstellt wurden und derzeit ausgeführt werden. Informationen zum Entfernen eines zuvor konfigurierten öffentlichen Schlüssels, der auf einer laufenden Instance gespeichert ist, finden Sie unter Verwalten von Schlüsseln, die auf einer Instance in Amazon Lightsail gespeichert sind.

Löschen eines Standardschlüssels und Erstellung eines neuen in der Lightsail-Konsole

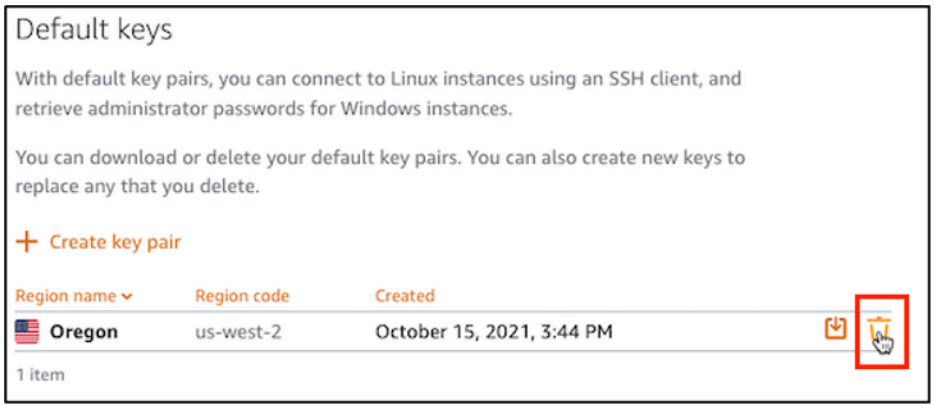
Vervollständigen Sie den folgenden Vorgang, um einen Standardschlüssel in der Lightsail-Konsole zu löschen. Dies verhindert, dass der Standardschlüssel für neue Instances konfiguriert wird, die Sie

in Lightsail erstellen. Sie können dann einen neuen Standardschlüssel erstellen, um den gelöschten Schlüssel zu ersetzen. Sie können den neuen Standardschlüssel für neue Instances konfigurieren, die Sie in Lightsail erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Homepage im oberen Navigationsbereich Account (Konto) aus.
3. Wählen Sie im Dropdown-Menü Konto aus.



4. Wählen Sie die Registerkarte SSH-Schlüssel aus.
5. Wählen Sie im Abschnitt Standardschlüssel der Seite das Löschsymbol für den Standardschlüssel, den Sie löschen möchten.

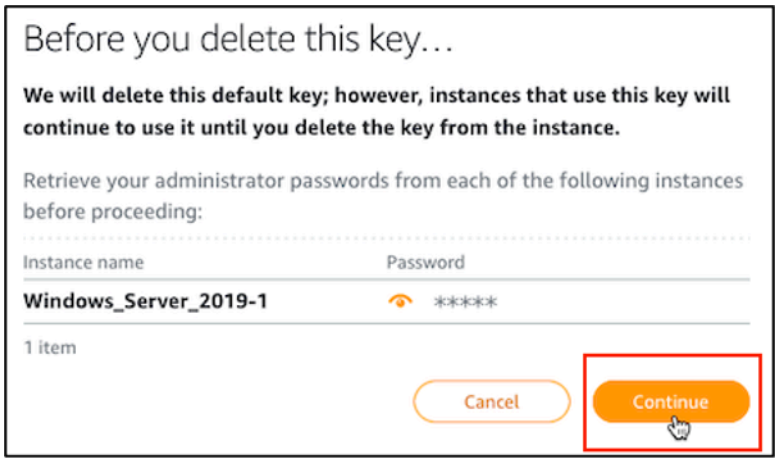


> **Important**
>
> Das Löschen eines Standardschlüssels entfernt den öffentlichen Schlüssel des benutzerdefinierten Schlüsselpaares nicht aus Instances, die zuvor erstellt wurden und derzeit ausgeführt werden. Weitere Informationen finden Sie unter Verwalten von Schlüsseln, die auf einer Instance in Amazon Lightsail gespeichert sind.

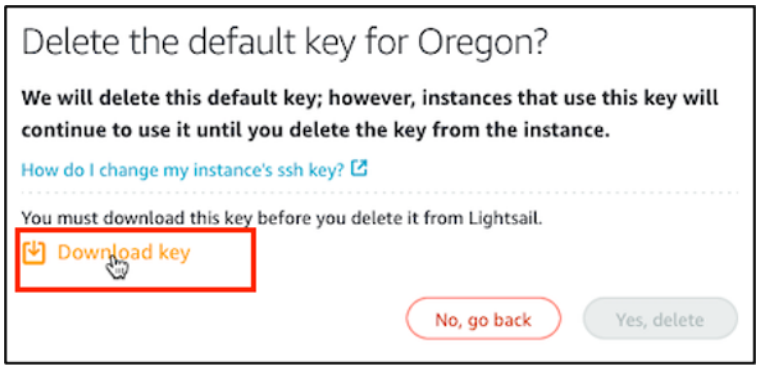
6. Der Standardschlüssel wird verwendet, um das Administratorkennwort für Windows-Instances zu generieren. Bevor Sie den Standardschlüssel löschen, sollten Sie das Administratorkennwort

von allen Windows-Instances abrufen und speichern, die den zu löschenden Standardschlüssel verwenden.

7. Wählen Sie Continue (Fortfahren), um den Standardschlüssel zu löschen.



8. Sie müssen den Standardschlüssel herunterladen, bevor Sie ihn löschen können. Nachdem Sie den Standardschlüssel heruntergeladen haben, können Sie Yes, delete (Ja, löschen) wählen, um den Standardschlüssel dauerhaft zu löschen.



9. Der Standardschlüssel wurde gelöscht. Klicken Sie auf Okay.

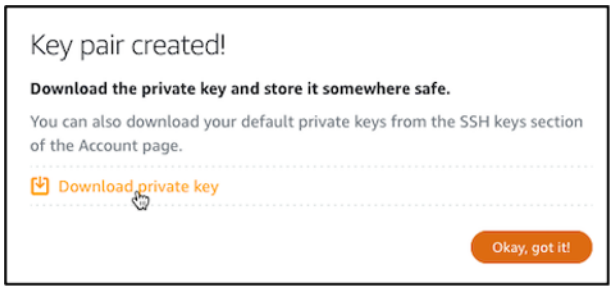
Die folgenden Schritte sind optional und Sie sollten sie nur ausführen, wenn Sie das gelöschte Standardschlüsselpaar ersetzen möchten.

10. Wählen Sie im Abschnitt Standardschlüssel der Seite Create key pair (Schlüsselpaar erstellen).

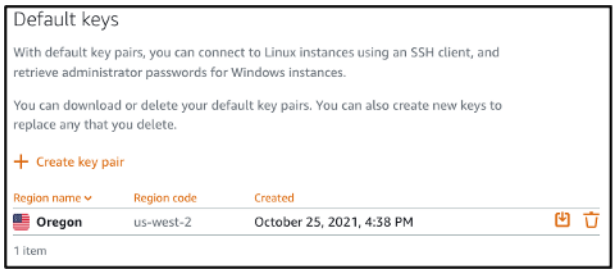
11. Wählen Sie in der Aufforderung Select a region (Region auswählen), die angezeigt wird, die AWS-Region, in die Sie Ihren neuen Standardschlüssel erstellen möchten. Sie können Ihren neuen Standardschlüssel auf neuen Instances im selben AWS-Region konfigurieren.

    > **Note**
    >
    > Mit diesen Schritten können Sie Standardschlüsselpaare nur in AWS-Regionen erstellen, in denen Sie Lightsail-Ressourcen erstellt haben. Um ein Standard-Schlüsselpaar in einer neuen Region zu erstellen, müssen Sie eine Lightsail-Ressource in dieser Region erstellen. Durch das Erstellen der Ressource wird auch ein Standardschlüsselpaar erstellt.

12. Laden Sie den privaten Schlüssel herunter und speichern Sie ihn an einem sicheren Ort.
13. Wählen Sie Ok, got it! (Ok, verstanden!), um fortzufahren.



14. Bestätigen Sie den neuen Standardschlüssel auf der Lightsail-Konsolenseite SSH-Schlüssel.

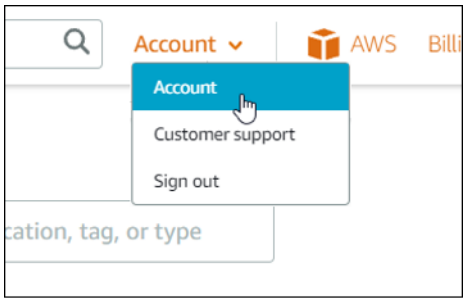


Sie können Ihre neuen Standardschlüssel für neue Instances konfigurieren, die Sie in Lightsail erstellen. Informationen zum Konfigurieren Ihres neuen Standardschlüssels für Instances, die zuvor erstellt wurden und derzeit ausgeführt werden, finden Sie unter Verwalten von Schlüsseln, die auf einer Instance in Amazon Lightsail gespeichert sind.

So erstellen Sie einen benutzerdefinierten Schlüssel mithilfe der Lightsail-Konsole

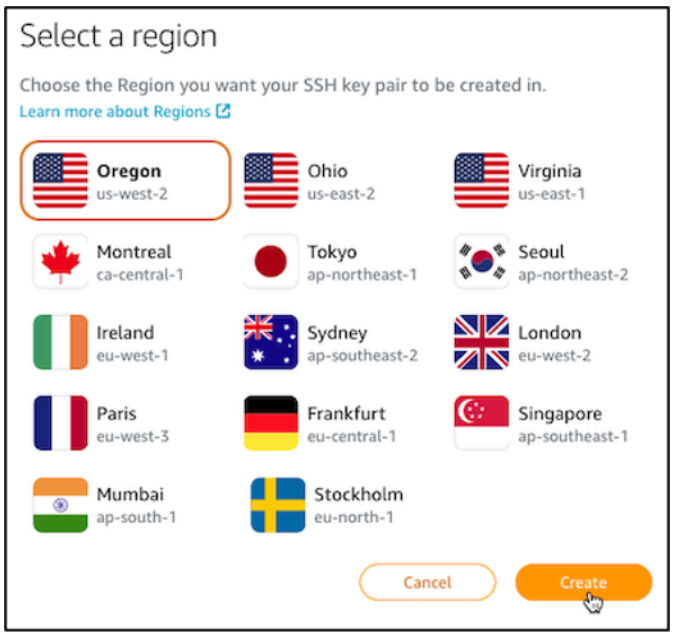
Führen Sie die folgenden Schritte aus, um ein benutzerdefiniertes Schlüsselpaar mithilfe der Lightsail-Konsole zu erstellen. Sie können den neuen benutzerdefinierten Schlüssel für neue Instances konfigurieren, die Sie in Lightsail erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Homepage im oberen Navigationsbereich Account (Konto) aus.
3. Wählen Sie im Dropdown-Menü Konto aus.

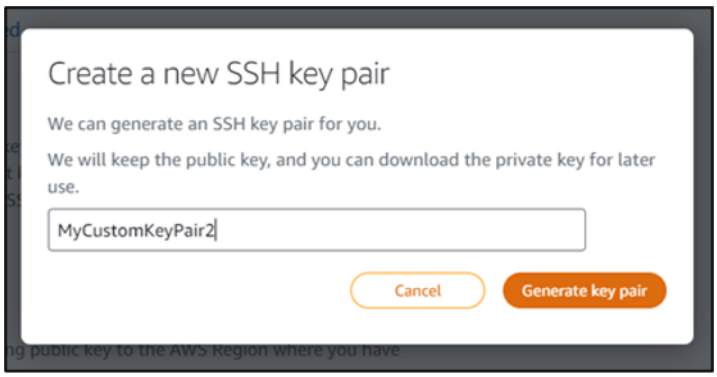


4. Wählen Sie die Registerkarte SSH-Schlüssel aus.
5. Wählen Sie Create key pair (Erstellen eines Schlüsselpaares) im Abschnitt Custom keys (Benutzerdefinierte Schlüssel) der Seite.

6. Wählen Sie in der Aufforderung Select a region (Region auswählen), die angezeigt wird, die AWS-Region, in die Sie Ihren neuen benutzerdefinierten Schlüssel erstellen möchten. Sie können Ihren neuen benutzerdefinierten Schlüssel auf neuen Instances im selben AWS-Region konfigurieren.



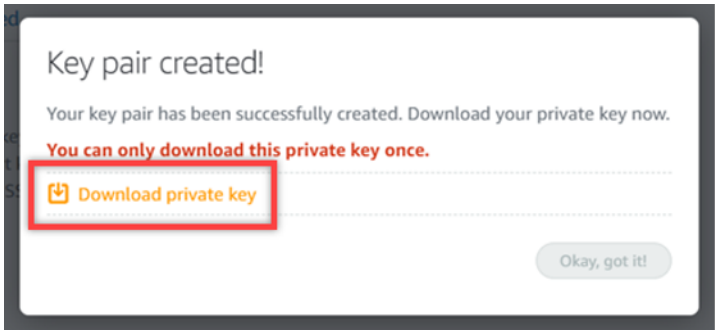
7. Geben Sie in der Aufforderung Create a new SSH key pair (Erstellen Sie ein neues SSH-Schlüsselpaar), die angezeigt wird, Ihrem benutzerdefinierten Schlüssel einen Namen und wählen Sie Generate key pair (Generieren von Schlüsselpaar).



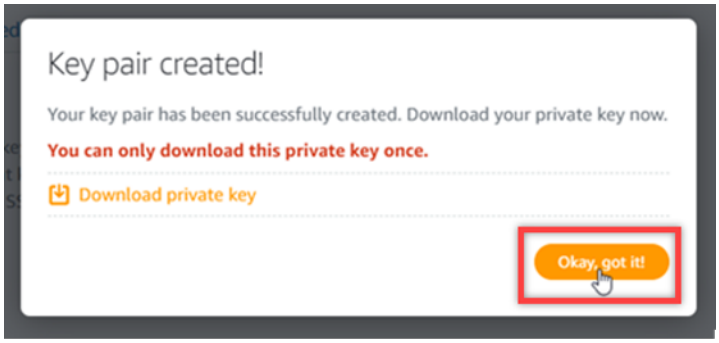
8. Wählen Sie in der Aufforderung Key pair created! (Schlüsselpaar ist erstellt!), die angezeigt wird, Download private key (Laden Sie den privaten Schlüssel herunter), um den privaten Schlüssel auf Ihrem lokalen Computer zu speichern.

> **Important**
>
> Speichern Sie den privaten Schlüssel an einem gesicherten Ort. Teilen Sie ihn nicht öffentlich, da er verwendet werden kann, um eine Verbindung zu Ihren Instances herzustellen.
>
> Dies ist der einzige Zeitpunkt, an dem Sie den privaten Schlüssel des benutzerdefinierten Schlüsselpaars herunterladen können. Lightsail speichert nicht den privaten Schlüssel

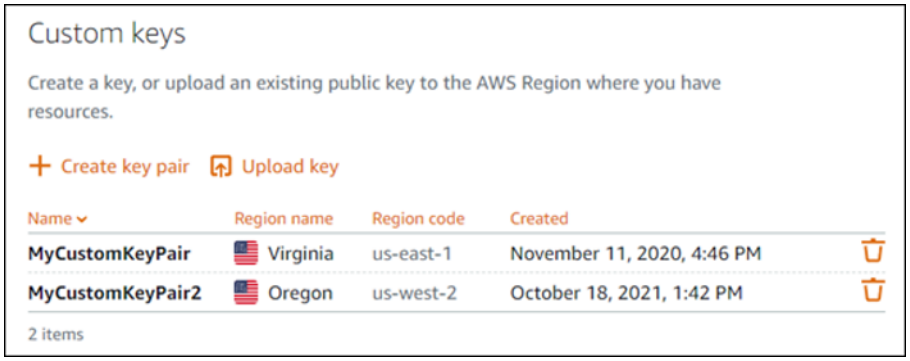
von benutzerdefinierten Schlüsselpaaren. Nachdem Sie diese Aufforderung geschlossen haben, können Sie ihn nicht mehr herunterladen.



9. Wählen Sie Ok, got it! (Ok, verstanden!), um die Aufforderung zu schließen.



10. Ihr neuer benutzerdefinierter Schlüssel ist im Abschnitt Benutzerdefinierte Schlüssel der Seite.



Sie können Ihre neuen benutzerdefinierten Schlüssel für neue Instances konfigurieren, die Sie in Lightsail erstellen, konfigurieren. Informationen zum Konfigurieren Ihres neuen benutzerdefinierten Schlüssels für Instances, die zuvor erstellt wurden und derzeit ausgeführt werden, finden Sie unter Verwalten von Schlüsseln, die auf einer Instance gespeichert sind Amazon Lightsail.

Erstellen eines benutzerdefinierten Schlüssels mit ssh-keygen und hochladen in Lightsail

Führen Sie das folgende Verfahren aus, um ein benutzerdefiniertes Schlüsselpaar auf Ihrem lokalen Computer mit einem Drittanbieter-Tool wie ssh-keygen zu erstellen. Nachdem Sie den Schlüssel erstellt haben, können Sie ihn in die Lightsail-Konsole hochladen. Sie können den neuen benutzerdefinierten Schlüssel für neue Instances konfigurieren, die Sie in Lightsail erstellen.

1. Öffnen Sie Eingabeaufforderung oder Terminal auf Ihrem lokalen Computer.
2. Geben Sie den folgenden Befehl ein, um ein neues Schlüsselpaar zu erstellen.

   ```
   ssh-keygen -t rsa
   ```

3. Geben Sie einen Verzeichnisspeicherort auf Ihrem Computer an, in dem das Schlüsselpaar gespeichert werden soll.

   Sie können z. B. eines der folgenden Verzeichnisse angeben:

   a. Bei Windows: `C:\Users\`*`<UserName>`*`\.ssh\`*`<KeyPairName>`

   b. Unter macOS, Linux oder Unix: `/home/`*`<UserName>`*`/.ssh/`*`<KeyPairName>`

   Ersetzen Sie *`<UserName>`* mit dem Namen des Benutzers, als den Sie derzeit angemeldet sind, und ersetzen Sie *`<KeyPairName>`* durch den Namen Ihres neuen Schlüsselpaares.

   Im folgenden Beispiel haben wir das `C:\Keys`-Verzeichnis auf unserem Windows-Computer angegeben und dem neuen Schlüssel den Namen `MyNewLightsailCustomKey` gegeben.

4. Geben Sie eine Passphrase für Ihren Schlüssel ein und drücken Sie Enter (Eingabe-Taste). Sie werden die Passphrase nicht sehen, wenn Sie sie eingeben.

   Sie benötigen diese Passphrase später, wenn Sie den privaten Schlüssel des Schlüsselpaares auf einem SSH-Client konfigurieren, um eine Verbindung zu einer Instance herzustellen, auf der der öffentliche Schlüssel des Schlüsselpaares konfiguriert ist.

5. Geben Sie die Passphrase erneut ein und klicken Sie auf Enter (Eingabe-Taste). Sie werden die Passphrase nicht sehen, wenn Sie sie eingeben.

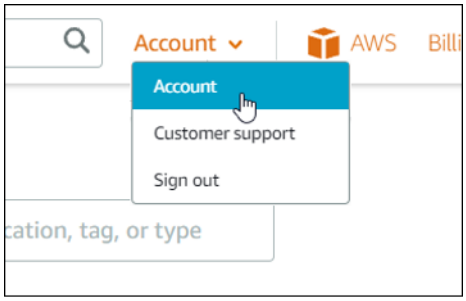
```
Enter same passphrase again:
```

6. Eine Aufforderung bestätigt, dass Ihr privater Schlüssel und Ihr öffentlicher Schlüssel im angegebenen Verzeichnis gespeichert wurden.

```
Your identification has been saved in C:\Keys\MyNewLighstailCustomKey.
Your public key has been saved in C:\Keys\MyNewLighstailCustomKey.pub.
```

Als Nächstes laden Sie den öffentlichen Schlüssel des Schlüsselpaares in die Lightsail-Konsole.

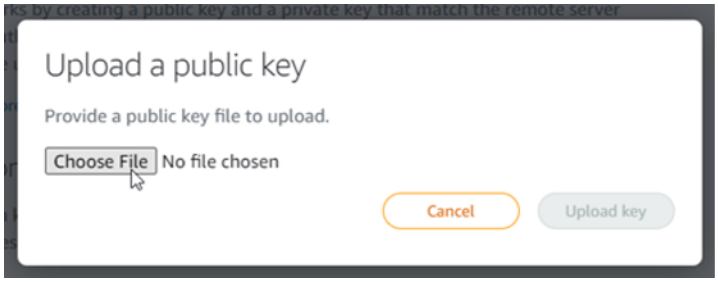
7. Melden Sie sich an der Lightsail-Konsole an.
8. Wählen Sie auf der Lightsail-Homepage im oberen Navigationsbereich Account (Konto) aus.
9. Wählen Sie im Dropdown-Menü Konto aus.



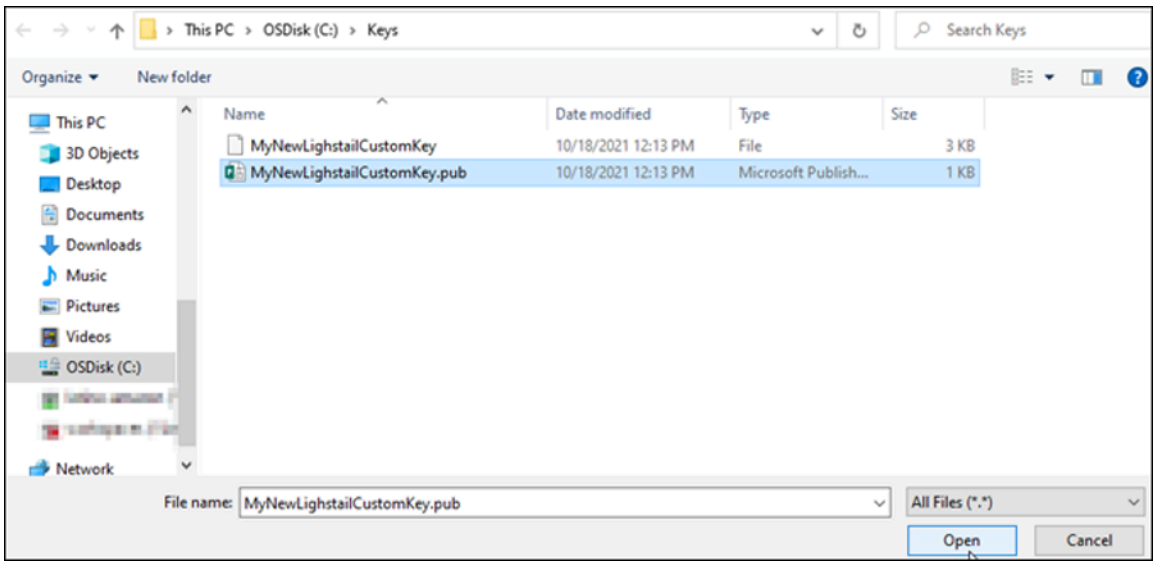
10. Wählen Sie die Registerkarte SSH-Schlüssel aus.
11. Wählen Sie Upload key (Schlüssel hochladen) im Abschnitt Benutzerdefinierte Schlüssel der Seite.

12. Wählen Sie in der Aufforderung Select a region (Region auswählen), die angezeigt wird, die AWS-Region, in die Sie Ihren neuen benutzerdefinierten Schlüssel hochladen möchten. Sie können Ihren neuen benutzerdefinierten Schlüssel auf neuen Instances im selben AWS-Region konfigurieren.

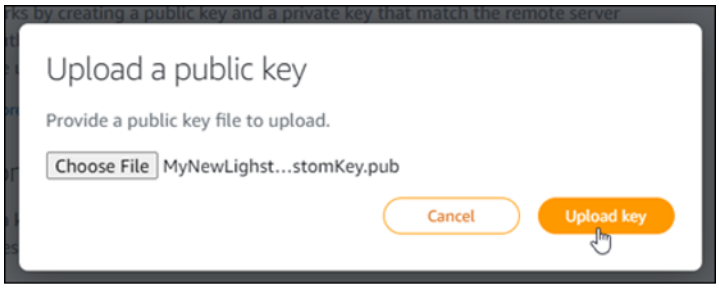
13. Klicken Sie auf Hochladen.
14. Klicken Sie in der Aufforderung Upload a public key (Einen öffentlichen Schlüssel hochladen), die erscheint, auf Choose File (Datei auswählen).



15. Suchen Sie den öffentlichen Schlüssel des Schlüsselpaares, den Sie zuvor in diesem Verfahren erstellt haben, auf Ihrem lokalen Computer und wählen Sie Open (Öffnen) aus. Der öffentliche Schlüssel des Schlüsselpaares ist die Datei mit der Dateierweiterung .PUB.



16. Klicken Sie auf Upload key (Schlüssel hochladen).



17. Ihr neuer benutzerdefinierter Schlüssel ist im Abschnitt Benutzerdefinierte Schlüssel der Seite.

Sie können Ihren neuen benutzerdefinierten Schlüssel für neue Instances konfigurieren, die Sie in der AWS-Region erstellen, in die Sie Ihren Schlüssel hochgeladen haben. Informationen zum Konfigurieren Ihres neuen benutzerdefinierten Schlüssels für Instances, die zuvor erstellt wurden und derzeit ausgeführt werden, finden Sie unter Verwalten von Schlüsseln, die auf einer Instance gespeichert sind Amazon Lightsail.

SSH-Schlüssel verwalten, die auf einer Lightsail-Instance gespeichert sind

Sie können mit Schlüsselpaaren eine sichere Verbindung zu Ihren Amazon Lightsail-Instances herstellen. Lightsail konfiguriert den öffentlichen Schlüssel eines Schlüsselpaars auf Ihrer Linux- oder Unix-Instance, wenn Sie sie zum ersten Mal erstellen. Sie verwenden den privaten Schlüssel des Schlüsselpaares, um sich bei Ihrer Instance zu authentifizieren, wenn Sie eine SSH-Verbindung zu ihr herstellen. Weitere Informationen zu Schlüsseln finden Sie unter Schlüsselpaare und verbinden zu Instances.

Nachdem Ihre Instance betriebsbereit ist, können Sie das Schlüsselpaar, das für die Verbindung mit Ihrer Instance verwendet wird, ändern, indem Sie einen neuen öffentlichen Schlüssel für die Instance hinzufügen oder den öffentlichen Schlüssel für die Instance ersetzen (Löschen des vorhandenen öffentlichen Schlüssels und Hinzufügen eines neuen Schlüssels). Dies kann aus den folgenden Gründen erforderlich sein:

- Falls ein Benutzer in Ihrer Organisation mithilfe eines separaten Schlüsselpaares Zugriff auf die Instance benötigt, können Sie den öffentlichen Schlüssel Ihrer Instance hinzufügen.
- Wenn Sie eine neue Instance sichern müssen, die aus dem Snapshot einer Instance erstellt wurde, die einen kompromittierten Schlüssel verwendet hat.
- Oder falls ein Benutzer eine Kopie des privaten Schlüssels besitzt und Sie verhindern möchten, dass er eine Verbindung zu Ihrer Instance herstellt (beispielsweise weil er Ihre Organisation verlassen hat), können Sie den öffentlichen Schlüssel für die Instance löschen und durch einen neuen ersetzen.

Um einen Schlüssel auf Ihrer Instance hinzuzufügen oder zu ersetzen, müssen Sie eine Verbindung zu Ihrer Instance herstellen können. Wenn Sie Ihren vorhandenen privaten Schlüssel verloren haben, können Sie sich mit dem Lightsail-Browser-basierten SSH-Client mit Ihrer Instance verbinden. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Linux- oder Unix-Instance.

Inhalt

Schritt 1: Informationen über den Prozess

Im Folgenden finden Sie die allgemeinen Schritte zum Hinzufügen und Entfernen von Schlüsseln in einer Instance. Wenn Sie einen Schlüssel aus Ihrer Instance entfernen möchten, ohne einen neuen Schlüssel hinzuzufügen, lesen Sie Schritt 5: Löschen von vorhandenen öffentlichen Schlüsseln aus Ihrer Instance weiter unten in diesem Leitfaden.

1. Erstellen Sie ein Schlüsselpaar – Um Ihrer Instance einen neuen Schlüssel hinzuzufügen, müssen Sie zuerst ein neues Schlüsselpaar erstellen. Sie können ein benutzerdefiniertes oder Standard-Schlüsselpaar mit der Lightsail-Konsole oder auf Ihrem lokalen Computer mit einem Drittanbieter-Tool wie ssh-Keygen erstellen. Beide Methoden erzeugen ein neues Schlüsselpaar, das aus einem öffentlichen und einem privaten Schlüssel besteht. Weitere Informationen finden Sie in Schritt 2: Erstellen eines Schlüsselpaares weiter unten in diesem Leitfaden.
2. Einen öffentlichen Schlüssel zu Ihrer Instance hinzufügen – Nachdem Sie ein Schlüsselpaar erstellt haben, stellen Sie über SSH eine Verbindung zu Ihrer Instance her und fügen den öffentlichen Schlüssel des Schlüsselpaares zu Ihrer Instance hinzu. Weitere Informationen finden Sie in Schritt 3: Hinzufügen eines öffentlichen Schlüssels zu Ihrer Instance weiter unten in diesem Leitfaden.
3. Testen, ob Sie mit dem neuen Schlüsselpaar eine Verbindung zu Ihrer Instance herstellen können – Nachdem der öffentliche Schlüssel des Schlüsselpaares in der Instance gespeichert wurde, sollten Sie testen, ob Sie den privaten Schlüssel des Schlüsselpaares verwenden können, um sich mit SSH mit der Instance zu verbinden. Weitere Informationen finden Sie in Schritt 4: Stellen Sie mittels des neuen Schlüsselpaares eine Verbindung mit Ihrer Instance her weiter unten in diesem Leitfaden.
4. Entfernung eines alten öffentlichen Schlüssels aus Ihrer Instance – Nachdem Sie sich mit dem neuen Schlüssel erfolgreich mit Ihrer Instance verbunden haben, können Sie einen alten öffentlichen Schlüssel aus der Instance entfernen. Führen Sie diesen Schritt aus, um zu verhindern, dass ein Benutzer über ein altes Schlüsselpaar eine Verbindung zu einer Instance herstellt. Weitere Informationen finden Sie in Schritt 5: Löschen von vorhandenen öffentliche Schlüsseln aus Ihrer Instance weiter unten in diesem Leitfaden.

Schritt 2: Erstellen eines Schlüsselpaares

Führen Sie das folgende Verfahren aus, um mit ssh-keygen ein Schlüsselpaar auf Ihrem lokalen Computer zu erstellen.

1. Öffnen Sie Eingabeaufforderung oder Terminal auf Ihrem lokalen Computer.

2. Geben Sie den folgenden Befehl ein, um ein neues Schlüsselpaar zu erstellen.

```
ssh-keygen -t rsa
```

3. Geben Sie einen Verzeichnisspeicherort auf Ihrem Computer an, in dem das Schlüsselpaar gespeichert werden soll.

   Beispiel:

   - Bei Windows: `C:\Users\<UserName>\.ssh\<KeyPairName>`
   - Unter macOS, Linux oder Unix: `/home/<UserName>/.ssh/<KeyPairName>`

   Ersetzen Sie *<UserName>* durch den Namen des Benutzers, als den Sie derzeit angemeldet sind, und ersetzen Sie *<KeyPairName>* durch den Namen Ihres neuen Schlüsselpaares.

   Im folgenden Beispiel haben wir das `C:\Keys`-Verzeichnis auf unserem Windows-Computer angegeben und dem neuen Schlüssel den Namen `MyNewLightsailCustomKey` gegeben.

```
C:\Users\[redacted]>ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\[redacted]/.ssh/id_rsa): C:\Keys\MyNewLighstailCustomKey
```

4. Geben Sie eine Passphrase für Ihren Schlüssel ein und drücken Sie Enter (Eingabe-Taste). Sie werden die Passphrase nicht sehen, wenn Sie sie eingeben.

   Sie benötigen diese Passphrase später, wenn Sie den privaten Schlüssel auf einem SSH-Client konfigurieren, um eine Verbindung zu einer Instance herzustellen, auf der der öffentliche Schlüssel konfiguriert ist.

```
Enter passphrase (empty for no passphrase):
```

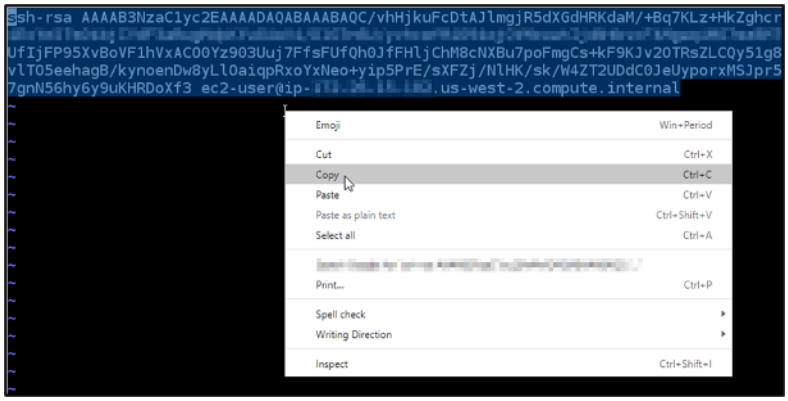
5. Geben Sie die Passphrase erneut ein und klicken Sie auf Enter (Eingabe-Taste). Sie werden die Passphrase nicht sehen, wenn Sie sie eingeben.

```
Enter same passphrase again:
```

6. Eine Aufforderung bestätigt, dass Ihr privater Schlüssel und Ihr öffentlicher Schlüssel im angegebenen Verzeichnis gespeichert wurden.

```
Your identification has been saved in C:\Keys\MyNewLighstailCustomKey.
Your public key has been saved in C:\Keys\MyNewLighstailCustomKey.pub.
```

7. Öffnen Sie die Datei (.PUB) des öffentlichen Schlüssels und kopieren Sie den Text in die Datei.

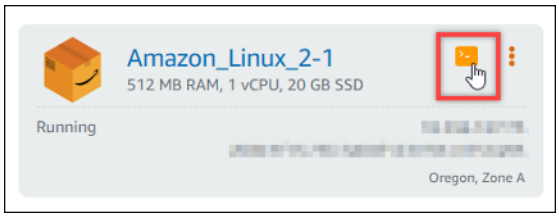


Fahren Sie mit dem nächsten Abschnitt dieses Leitfadens fort, um Ihren neuen öffentlichen Schlüssel zu Ihrer Lightsail-Instance hinzuzufügen.

Schritt 3: Hinzufügen eines öffentlichen Schlüssels zu Ihrer Instance

Führen Sie die folgenden Schritte aus, um den öffentlichen Schlüssel zu Ihrer Instance hinzuzufügen. Der Inhalt des öffentlichen Schlüssels wird in der Datei `~/.ssh/authorized_keys` auf Linux- und Unix-Instances gespeichert.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie die Registerkarte Instances auf der Startseite Lightsail.
3. Wählen Sie das browserbasierte SSH-Clientsymbol für die Instance aus, mit der Sie eine Verbindung herstellen möchten.



4. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um die authorized_keys-Datei mit dem Texteditor Ihrer Wahl zu bearbeiten. Die folgenden Schritte verwenden Vim zu Demonstrationszwecken.

```
sudo vim ~/.ssh/authorized_keys
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten, das die aktuellen öffentlichen Schlüssel anzeigt, die für Ihre Instance konfiguriert sind. In unserem Fall ist der Lightsail-

Standardschlüssel für die AWS-Region, in der die Instance erstellt wurde, er einzige öffentliche Schlüssel, der für die Instance konfiguriert wurde.

5. Drücken Sie die Taste I, um in den Einfügemodus im Vim-Editor zu gelangen.
6. Geben Sie einen Zeilenumbruch nach dem letzten öffentlichen Schlüssel in der Datei ein.
7. Fügen Sie den Text des öffentlichen Schlüssels ein, den Sie zuvor in diesem Leitfaden kopiert haben (nachdem Sie ein neues Schlüsselpaar erstellt haben). Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

8. Drücken Sie die Taste ESC. Geben Sie als Nächstes `:wq!` ein und drücken Sie Enter (Eingabe-Taste), um Ihre Bearbeitungen zu speichern und den Vim-Editor zu beenden.

Der neue öffentliche Schlüssel ist nun zu Ihrer Instance hinzugefügt. Fahren Sie mit dem nächsten Abschnitt dieses Leitfadens fort, um mithilfe des neuen Schlüsselpaares eine Verbindung zu Ihrer Instance herzustellen.

Schritt 4: Stellen Sie mittels des neuen Schlüsselpaares eine Verbindung mit Ihrer Instance her

Um das neue Schlüsselpaar zu testen, trennen Sie die Verbindung zu Ihrer Instance, und stellen Sie erneut eine Verbindung mit dem privaten Schlüssel her, das Sie zuvor in diesem Leitfaden erstellt haben. Weitere Informationen finden Sie unter Schlüsselpaare und Herstellung einer Verbindung zu Instances in Amazon Lightsail. Nachdem Sie sich mit dem neuen Schlüssel erfolgreich mit Ihrer Instance verbunden haben, können Sie einen alten Schlüssel aus der Instance entfernen. Fahren Sie mit dem nächsten Schritt fort, um zu erfahren, wie Sie öffentliche Schlüssel aus Ihrer Instance löschen.

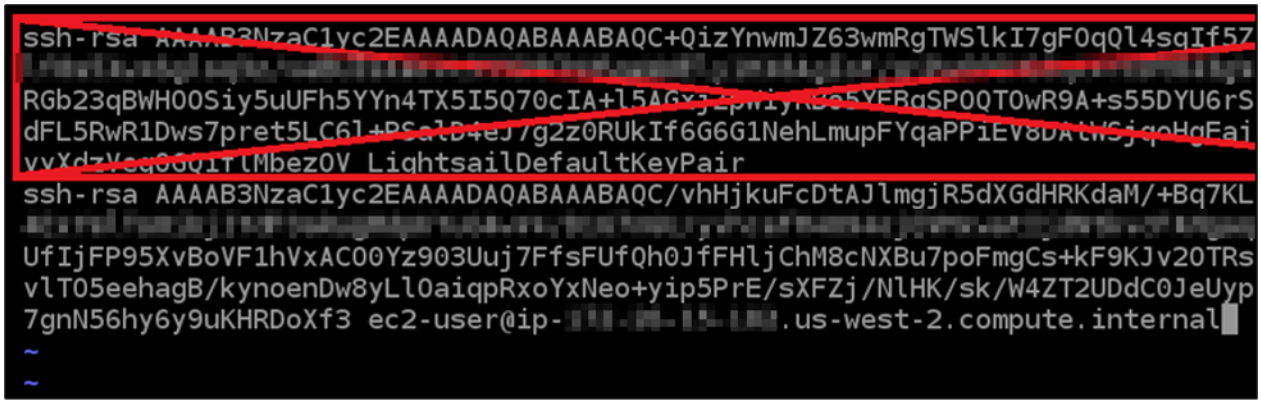
Schritt 5: Löschen von vorhandenen öffentliche Schlüsseln aus Ihrer Instance

Führen Sie die folgenden Schritte aus, um einen öffentlichen Schlüssel aus Ihrer Instance zu entfernen. Dies verhindert, dass ein Benutzer über ein altes Schlüsselpaar eine Verbindung zu einer Instance herstellt. Tun Sie dies, nachdem Sie sich mit dem neuen Schlüsselpaar erfolgreich mit der Instance verbunden haben.

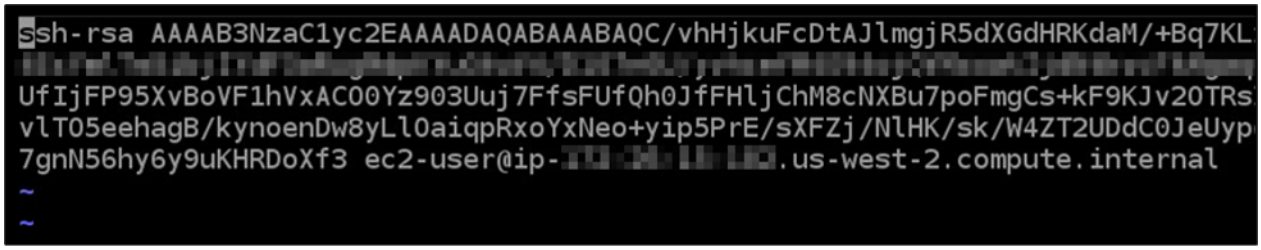
1. Stellen Sie per SSH eine Verbindung zu Ihrer -Instance her.
2. Geben Sie den folgenden Befehl ein, um die authorized_keys-Datei mit dem Texteditor Ihrer Wahl zu bearbeiten. Die folgenden Schritte verwenden Vim zu Demonstrationszwecken.

   ```
   sudo vim ~/.ssh/authorized_keys
   ```

3. Drücken Sie den Buchstaben I, um in den Einfügemodus im Vim-Editor zu gelangen.
4. Löschen Sie die Textzeile, die den öffentlichen Schlüssel enthält, den Sie aus Ihrer Instance entfernen möchten.

   Das Ergebnis sollte wie im folgenden Beispiel aussehen, in dem der neue öffentliche Schlüssel der einzige Schlüssel ist, der angezeigt wird.

5. Drücken Sie die Taste ESC. Geben Sie als Nächstes `:wq!` ein und drücken Sie Enter (Eingabe-Taste), um Ihre Bearbeitungen zu speichern und den Vim-Editor zu beenden.

Der gelöschte öffentliche Schlüssel ist nun aus Ihrer Instance entfernt. Ihre Instance wird Verbindungen verweigern, die den privaten Schlüssel dieses Schlüsselpaares verwenden.

PuTTY für Lightsail herunterladen und einrichten

Sie können einen SSH-Client wie PuTTY verwenden, um eine Verbindung zu Ihrer Lightsail-Instance herzustellen. PuTTY erfordert eine Kopie Ihres privaten SSH-Schlüssels. Möglicherweise haben Sie bereits einen Schlüssel oder Sie möchten möglicherweise das Schlüsselpaar verwenden, das Lightsail erstellt. In jedem Fall haben wir die Lösung für Sie. Weitere Informationen zu SSH finden Sie unter SSH-Schlüsselpaare. In diesem Thema erfahren Sie schrittweise, wie Sie ein Schlüsselpaar herunterladen und PuTTY einrichten, um eine Verbindung zu Ihrer Instance herzustellen.

Die in diesem Leitfaden beschriebene Methode zum Herstellen einer Verbindung mit Ihrer Instance ist eine von vielen. Weitere Informationen zu anderen Methoden finden Sie unter SSH-Schlüsselpaare.

Die einfachste Möglichkeit, eine Verbindung zu Ihrer Linux- oder Unix-Instance in Lightsail herzustellen, ist die Verwendung des browserbasierten SSH-Clients, der in der Lightsail-Konsole verfügbar ist. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Linux- oder Unix-Instance in Amazon Lightsail.

Voraussetzungen

- Sie benötigen eine laufende Instance in Lightsail. Weitere Informationen finden Sie unter Erstellen einer Instance in Amazon Lightsail.
- Wir empfehlen Ihnen, eine statische IP-Adresse zu erstellen und an Ihre Instance anzufügen, damit Sie PuTTY nicht neu konfigurieren müssen, wenn sich Ihre öffentliche IP-Adresse später ändert. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

Schritt 1: Laden Sie PuTTy herunter und installieren Sie es

PuTTY ist eine kostenlose Implementierung von SSH für Windows. Erfahren Sie mehr über PuTTY auf der PuTTY-Website, einschließlich Einschränkungen in Bezug auf Länder, in denen die Verschlüsselung nicht zulässig ist. Wenn Sie PuTTY bereits besitzen, können Sie mit Step 2 (Schritt 2) fortfahren.

1. Laden Sie das PuTTY-Installationsprogramm oder eine ausführbare Datei über den folgenden Link herunter: PuTTY herunterladen.

Wenn Sie Hilfe bei der Auswahl des Downloads benötigen, lesen Sie in der PuTTY-Dokumentation nach. Wir empfehlen die Verwendung der neuesten Version.

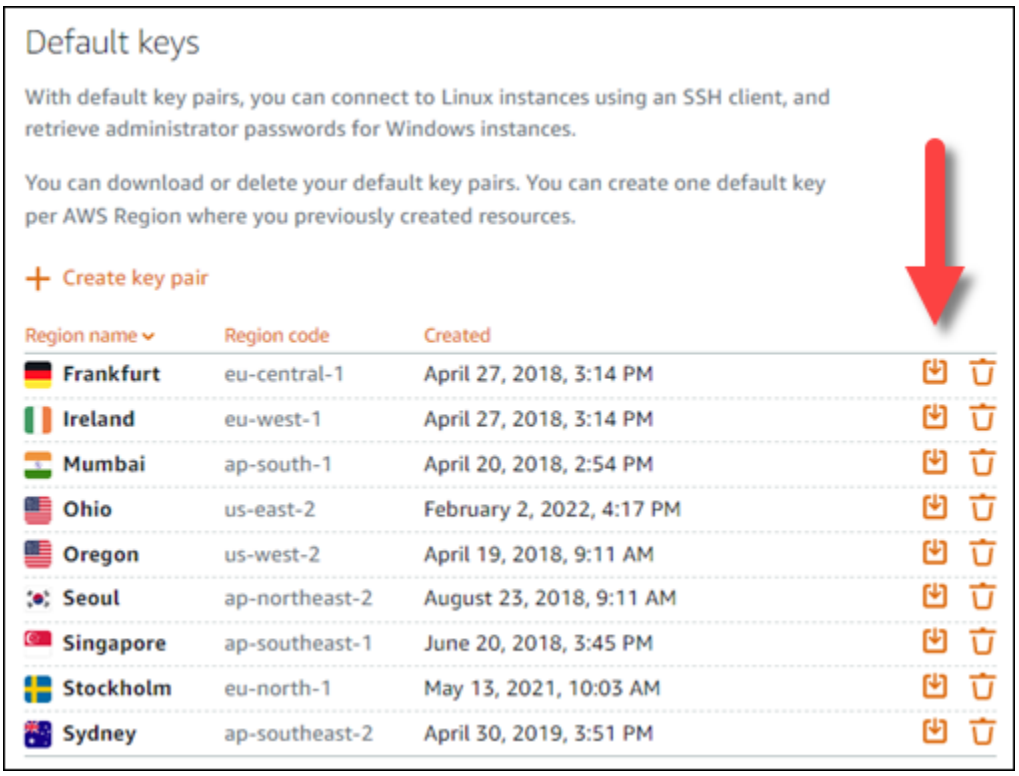
2. Fahren Sie mit Step 2 (Schritt 2) fort, um Ihren privaten Schlüssel zu erhalten, bevor Sie PuTTY konfigurieren.

Schritt 2: Halten Sie Ihren privaten Schlüssel bereit

Es gibt mehrere Möglichkeiten, einen privaten Schlüssel zu erhalten. Möglicherweise möchten Sie den von Lightsail generierten privaten Standardschlüssel verwenden, Lightsail einen neuen privaten Schlüssel für Sie erstellen lassen oder bereits einen von einem anderen Service haben. Die Schritte für jede dieser Optionen werden in den folgenden Verfahren beschrieben:

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie in der oberen Navigationsleiste Account (Konto) und dann Account (Konto) aus der Dropdown-Liste.
3. Wählen Sie die Registerkarte SSH Keys (SSH-Schlüssel) aus.
4. Wählen Sie eine der folgenden Optionen, je nachdem, welchen privaten Schlüssel Sie bevorzugen:

   - Um den privaten Standardschlüssel zu verwenden, den Lightsail generiert, wählen Sie im Abschnitt Standardschlüssel der Seite das Download-Symbol neben dem privaten Standardschlüssel für die aus, AWS-Region in der sich Ihre Instance befindet.



- Um ein neues Schlüsselpaar in Lightsail zu erstellen, wählen Sie im Abschnitt Benutzerdefinierte Schlüssel der Seite die Option Schlüsselpaar erstellen aus. Wählen Sie die aus, AWS-Region in der sich Ihre Instance befindet, und wählen Sie Erstellen aus. Geben Sie einen Namen ein und wählen Sie Generate key pair (Schlüsselpaar generieren). Sie haben die Möglichkeit, den neuen privaten Schlüssel herunterzuladen.

  > **Important**
  >
  > Sie können den privaten Schlüssel nur einmal herunterladen. Speichern Sie ihn an einem sicheren Ort.

- Um Ihren eigenen privaten Schlüssel zu verwenden, wählen Sie Upload New (Neuen Schlüssel hochladen). Wählen Sie die aus, AWS-Region in der sich Ihre Instance befindet, und wählen Sie Hochladen aus. Wählen Sie Upload file (Datei hochladen), und suchen Sie die Datei auf Ihrem lokalen Laufwerk. Wählen Sie Schlüssel hochladen, wenn Sie bereit sind, Ihre Datei mit dem öffentlichen Schlüssel in Lightsail hochzuladen.

5. Wenn Sie den privaten Schlüssel heruntergeladen oder einen neuen privaten Schlüssel in Lightsail erstellt haben, stellen Sie sicher, dass Sie die `.pem` Schlüsseldatei an einer beliebigen Stelle speichern, an der Sie sie leicht finden können.

Wir empfehlen Ihnen auch, die Berechtigungen für die Datei so einzustellen, dass niemand sonst sie lesen kann.

Schritt 3: Konfigurieren von PuTTYgen mit Ihrem privaten Lightsail-Schlüssel

Nachdem Sie eine Kopie Ihrer `.pem` Schlüsseldatei haben, können Sie PuTTY mithilfe des PuTTY Key Generator (PuTTYgen) einrichten.

1. Starten Sie PuTTYgen (z. B. indem Sie im Start-Menü All Programs (Alle Programme), PuTTY, PuTTYgen wählen).
2. Wählen Sie Laden aus.

   PuTTYgen zeigt standardmäßig nur Dateien mit der Erweiterung `.ppk` an. Wählen Sie die Option zum Anzeigen aller Dateitypen aus, damit Ihre `.pem`-Datei angezeigt wird.
3. Wählen Sie `lightsailDefaultKey.pem` und klicken Sie auf Open (Öffnen).

   PuTTYgen bestätigt, dass Sie den Schlüssel erfolgreich importiert haben, klicken Sie dann auf OK.
4. Wählen Sie Save private key (Privaten Schlüssel speichern) und bestätigen Sie, dass Sie ihn nicht mit einer Passphrase speichern möchten.

   Wenn Sie eine Passphrase als zusätzliche Sicherheitsmaßnahme erstellenwollen, denken Sie daran, dass Sie sie jedes Mal eingeben müssen, wenn Sie eine Verbindung mit Ihrer Instance mithilfe von PuTTY herstellen.
5. Geben Sie einen Namen und einen Speicherort für Ihren privaten Schlüssel an, und wählen Sie anschließend Save (Speichern).
6. Schließen Sie PuTTygen.

Schritt 4: Konfigurieren Sie PuTTY mit Ihrem privaten Schlüssel und Instance-Informationen

Fast geschafft! Wir müssen nur noch eine letzte Änderung vornehmen.

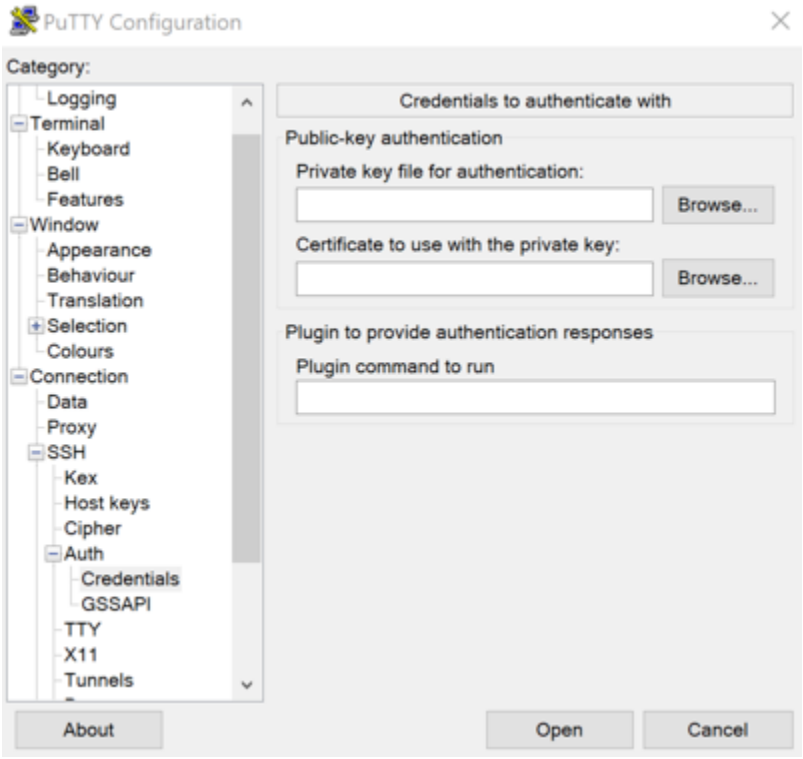
1. Öffnen Sie PuTTY.
2. Rufen Sie von Lightsail aus die öffentliche IP-Adresse (Hoffentlich verwenden Sie eine statische IP-Adresse) auf der Instance-Verwaltungsseite ab.

Sie können die öffentliche IP-Adresse von der Lightsail-Startseite abrufen oder Ihre Instance auswählen, um weitere Details dazu anzuzeigen.

3. Geben (oder fügen) Sie die öffentliche IP-Adresse in das Feld Host Name (or IP address) (Hostname (oder IP-Adresse)) ein.

> **Note**
>
> Port 22 ist bereits für SSH auf Ihrer Lightsail-Instance geöffnet. Akzeptieren Sie daher den Standardport.

4. Erweitern Sie unter Verbindung die Optionen SSH und Auth und wählen Sie anschließend Anmeldeinformationen.



5. Wählen Sie Browse (Durchsuchen), um zur `.ppk`-Datei zu gelangen, die Sie im vorherigen Schritt erstellt haben, und klicken Sie dann auf Open (Öffnen).
6. Klicken Sie erneut auf Öffnen, und wählen Sie dann Annehmen, um dieser Verbindung in Zukunft zu vertrauen.
7. Melden Sie sich je nach Betriebssystem Ihrer Instance mit einem der folgenden Standardbenutzernamen an:

- AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, FreeBSD und openSUSE-Instances: `ec2-user`
- CentOS-7-Instances: `centos`
- Debian-Instances: `admin`
- Ubuntu-Instances: `ubuntu`
- Bitnami-Instances: `bitnami`
- Plesk-Instances: `ubuntu`
- cPanel & WHM-Instances: `centos`

Weitere Informationen zu den Instance-Betriebssystemen finden Sie unter Auswählen eines Images.

8. Speichern Sie die Verbindung für die künftige Nutzung.

Nächste Schritte

Wenn Sie erneut eine Verbindung einrichten müssen, lesen Sie unter Verbindung mit Ihrer Linux/Unix-basierten Instance unter Verwendung von PuTTY.

Herstellen einer Verbindung mit Ihrer Lightsail-Windows-Instance

Sie können sich mit Ihrer Windows Server-Instance in Amazon Lightsail über den browserbasierten RDP-Client verbinden, der in der Lightsail-Konsole verfügbar ist. Für den browserbasierten RDP-Client ist keine Software-Installation erforderlich. Sie können sofort nach der Erstellung eine Verbindung zu Ihrer Windows Server-Instance herstellen, und sie wird verfügbar. Verbinden Sie sich mit Ihrer Instance, um administrative Aufgaben auf dem Server auszuführen, z. B. die Installation von Software oder die Konfiguration von Webanwendungen.

> **Important**
>
> Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um über IPv6 SSH oder RDP in Ihre Instance zu senden. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

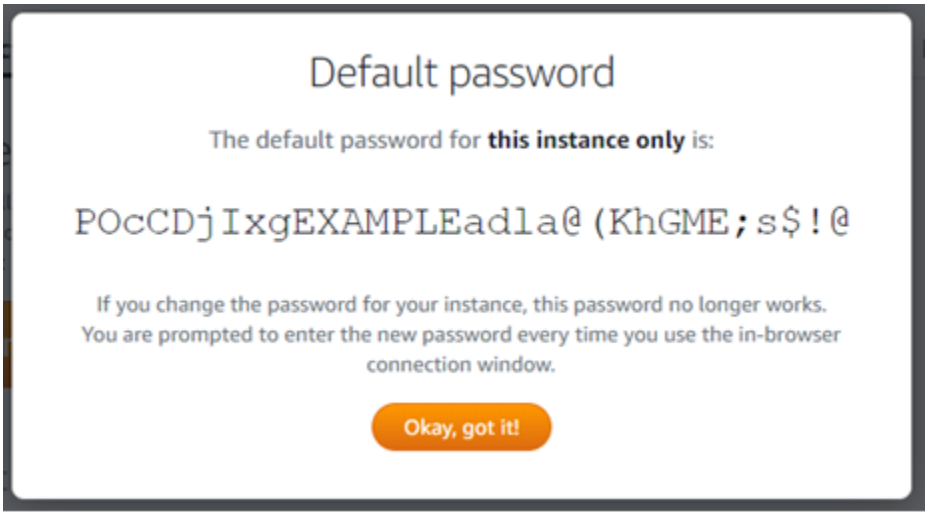
Sie können auch Ihren eigenen RDP-Client verwenden, um eine Verbindung zu Ihrer Instance herzustellen, z. B. den Client Remote Desktop Connection, der mit Windows gebündelt ist. Weitere Informationen zur Konfiguration Ihres eigenen RDP-Clients finden Sie unter Verbinden mit Ihrer Windows-Instance über den Remote Desktop Connection Client. Informationen zum Herstellen einer Verbindung mit einer Linux- oder Unix-Instance in Lightsail finden Sie unter Herstellen einer Verbindung mit Ihrer Linux- oder Unix-Instance.

Standard-Administratorpasswort für Windows Server-Instances

Beim Erstellen wird Windows Server-Instances ein zufällig generiertes Standard-Administratorpasswort zugewiesen. Der browserbasierte RDP-Client in der Lightsail-Konsole verwendet das Standard-Administratorpasswort, um sich bei Ihrer Instance anzumelden. Wenn Sie das Administratorpasswort für Ihrer Instance ändern, werden Sie jedes Mal, wenn Sie versuchen, eine Verbindung zu Ihrer Instance über den Browser-basierten RDP-Client herzustellen, aufgefordert, Ihr neues Passwort manuell einzugeben. Lightsail speichert Ihr neues Administratorpasswort nicht und es kann nicht von Ihrer Instance abgerufen werden.

> **Important**
>
> Wenn Sie Ihr Administratorpasswort verlieren, können Sie sich nicht mehr bei Ihrer Instance anmelden. Es gibt keine Möglichkeit, das Passwort zurückzusetzen. Speichern Sie Ihr neues Administratorpasswort an einem sicheren Ort, an dem Sie es später abrufen können, wenn Sie es verlieren, z. B. AWS Secrets Manager. Weitere Informationen finden Sie im AWS Secrets Manager-Benutzerhandbuch.

Sie können das Administratorpasswort wieder in das ursprüngliche Standard-Administratorpasswort ändern, um zu vermeiden, dass Sie bei jedem Zugriff auf die Instance über den browserbasierten RDP-Client dazu aufgefordert werden. Sie finden das ursprüngliche Standard-Administratorpasswort, indem Sie auf der Lightsail-Startseite die Registerkarte Instances auswählen. Wählen Sie den Namen Ihrer Windows-Server-Instance, klicken Sie auf die Registerkarte Connect (Verbinden) und wählen Sie Show default password (Standardpasswort anzeigen), um sich das ursprüngliche Standard-Administratorpasswort wie im folgenden Beispiel anzeigen zu lassen.

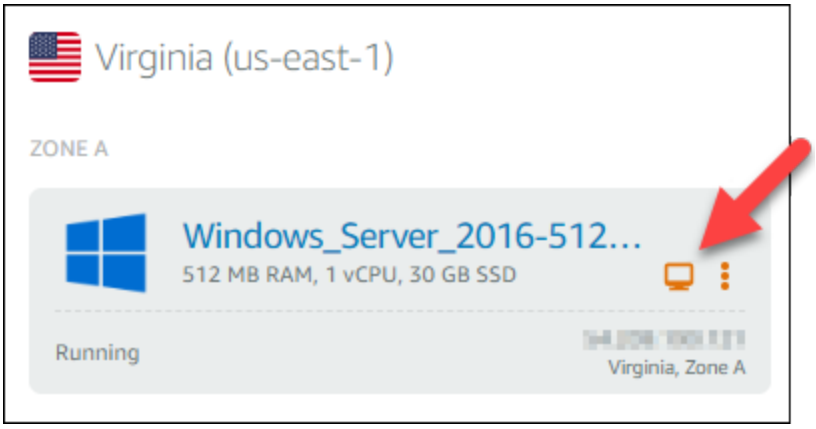


Herstellen einer Verbindung mit der Windows Server-Instance mithilfe des browserbasierten -RDP-Clients

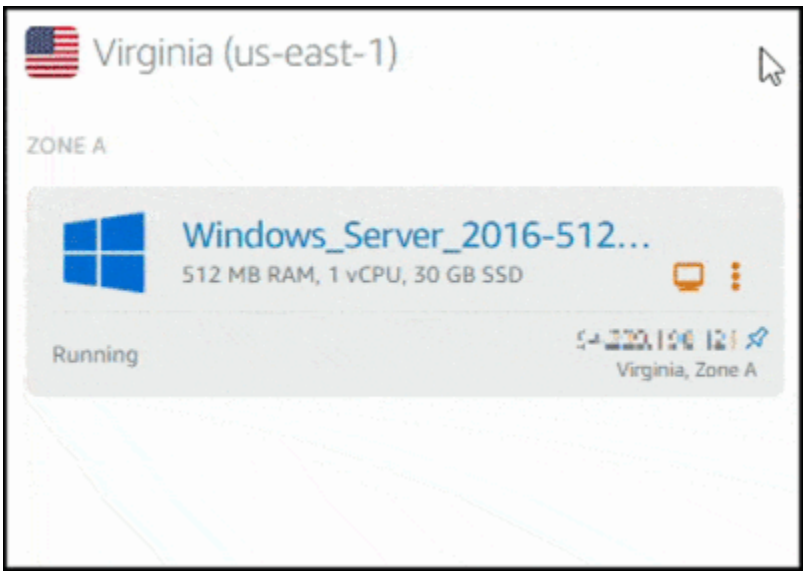
Gehen Sie wie folgt vor, um über den browserbasierten RDP-Client in der Lightsail-Konsole eine Verbindung zu Ihrer Windows Server-Instance herzustellen.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Rufen Sie den browserbasierten RDP-Client für die Instance auf, mit der Sie sich verbinden möchten, indem Sie einen der folgenden Schritte ausführen:

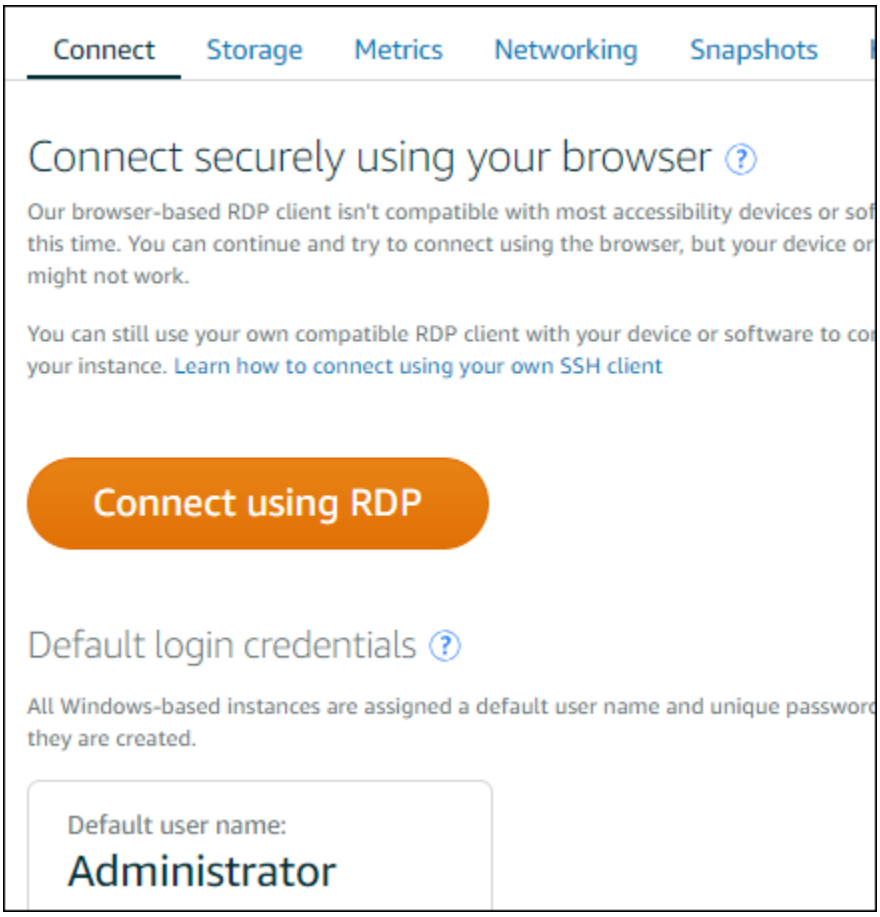
   - Klicken Sie auf das browserbasierte RDP-Client-Symbol, wie im folgenden Beispiel gezeigt:



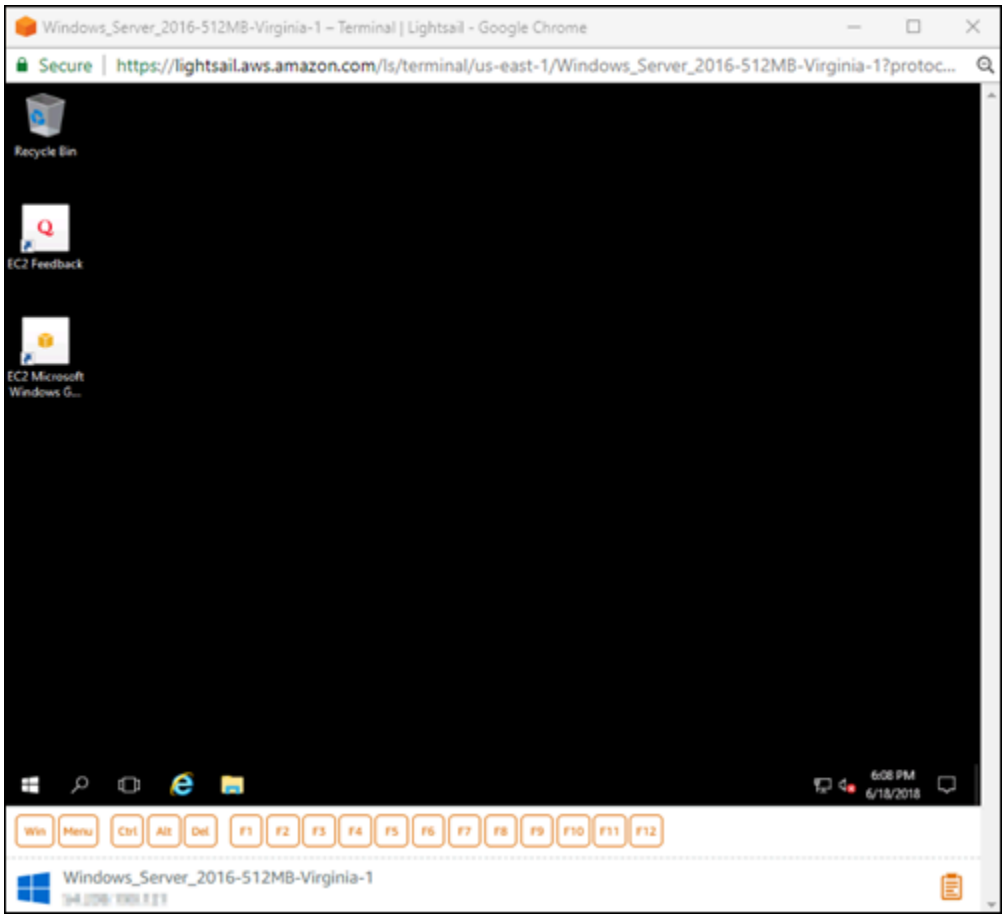
   - Wählen Sie das Menü „Aktionen“ (⋮) und klicken Sie dann auf Verbinden, wie im folgenden Beispiel gezeigt.



- Wählen Sie den Namen der Instance und wählen Sie auf der Registerkarte Connect (Verbinden) die Option Connect using RDP (Verbinden mit RDP).



Sie können die Interaktion mit Ihrer Instance beginnen, wenn sich der browserbasierte RDP-Client öffnet und ein Windows-Desktop angezeigt wird, wie im folgenden Beispiel gezeigt.



> **Note**
>
> Die Registerkarte Connect (Verbinden) bietet auch die erforderlichen Informationen, um eine Verbindung mit Ihrem eigenen RDP-Client herzustellen, z. B. den Standard-Benutzernamen und das Passwort für Ihre Windows-Instance. Weitere Informationen zum Konfigurieren Ihres eigenen RDP-Clients finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-Instance in Amazon Lightsail mithilfe des Remote Desktop Connection Clients.

Interagieren Sie mit Ihrer Windows-Instance über den browserbasierten RDP-Client.

Verwenden Sie den browserbasierten RDP-Client wie Ihren eigenen lokalen Windows-Desktop. RDP enthält Funktionstasten und andere Windows-spezifische Tasten, die Ihnen bei der Interaktion mit Ihrer Instance helfen. In den folgenden Abschnitten erfahren Sie, wie Sie in RDP Text in die Zwischenablage kopieren und aus der Zwischenablage einfügen.

So fügen Sie Text in den browserbasierten RDP-Client ein

1. Markieren Sie Text in Ihrem lokalen Desktop, drücken Sie dann Ctrl+C (STRG+C) oder Cmd+C, um ihn in Ihre lokale Zwischenablage zu kopieren.
2. Wählen Sie in der rechten unteren Ecke des browserbasierten RDP-Clients das Zwischenablagesymbol. Das Textfeld der browserbasierten RDP-Client-Zwischenablage wird angezeigt.
3. Klicken Sie in das Textfeld und drücken Sie dann Ctrl+V (STRG+V) oder Cmd+V,, um den Inhalt aus Ihrer lokalen Zwischenablage in die browserbasierte RDP-Client-Zwischenablage einzufügen.
4. Klicken Sie mit der rechten Maustaste auf einen beliebigen Bereich auf dem Remote-Desktop-Bildschirm, um den Text aus der Zwischenablage des browserbasierten RDP-Client auf dem Remote-Desktop-Bildschirm einzufügen.

So kopieren Sie Text vom browserbasierten RDP-Client

1. Markieren Sie Text auf dem Remote-Desktop-Bildschirm.
2. Wählen Sie in der rechten unteren Ecke des browserbasierten RDP-Clients das Zwischenablagesymbol. Das Textfeld der browserbasierten RDP-Client-Zwischenablage wird angezeigt.
3. Markieren Sie den Text, den Sie kopieren möchten, drücken Sie dann Ctrl+C (STRG+C) oder Cmd+C, um den Text in Ihre lokale Zwischenablage zu kopieren. Sie können den kopierten Text nun an beliebiger Stelle auf Ihrem lokalen Desktop einfügen.

Das Administratorpasswort für eine Lightsail-Windows-Instance ändern

Beim Erstellen einer Windows-Server-basierten Lightsail-Instance verwenden wir das Standardpasswort für die AWS-Region, in der die Instance erstellt wird. Dadurch ist es einfacher, eine Verbindung über einen Browser-basierten Remote-Desktop-Client (RDP) oder mithilfe eines Clients – wie z. B. Remote Desktop Connection – herzustellen.

> **Important**
>
> Wir empfehlen Ihnen dringend, das Passwort für Ihre Instance von Lightsail generieren zu lassen. Da wir Ihr benutzerdefiniertes Passwort nicht speichern, können Sie den Zugriff auf Ihre Lightsail-Instance verlieren, wenn Sie das Administratorpasswort ändern.

Ändern Ihres Administratorpassworts mithilfe von Windows Server

Sie können Ihr Administratorpasswort mithilfe des Windows Server-Tools Change Password (Passwort ändern) ändern. Geben Sie auf der Windows Server-basierten Lightsail-Instance `Ctrl` + `Alt` + `Del` ein und wählen Sie Change a password (Ein Passwort ändern) aus.

Entschlüsseln Ihres Schlüssels

Wenn Sie das Passwort für die Windows Server-basierte Lightsail-Instance ändern, können Sie die AWS Command Line Interface (AWS CLI) verwenden, um Informationen abzurufen, mit deren Hilfe Sie Ihr Passwort entschlüsseln.

Abrufen des Verschlüsselungstexts mithilfe der AWS CLI

1. Falls noch nicht erfolgt, installieren und konfigurieren Sie die AWS CLI.

   Weitere Informationen finden Sie unter Konfigurieren der AWS Command Line Interface für die Arbeit mit Amazon Lightsail.
2. Öffnen Sie eine Eingabeaufforderung oder ein Terminal-Fenster.
3. Geben Sie den folgenden Befehl ein:

   ```
   aws lightsail get-instance-access-details --instance-name my-instance
   ```

   Wobei *my-instance* der Name der Instance ist, über die Sie Informationen abrufen möchten.

   Die Ausgabe sieht in etwa wie die folgende aus.

   ```
   {
       "accessDetails": {
           "username": "Administrator",
           "protocol": "rdp",
           "ipAddress": "12.345.678.910",
           "passwordData": {
               "ciphertext": "cipher",
               "keyPairName": "my-ohio-key"
           },
           "password": "",
           "instanceName": "2016-ohio-windows"
       }
   }
   ```
4. Sie können den Verschlüsselungstext mit jeder verfügbaren Anwendung zum Entschlüsseln des Passworts verwenden.

Stellen Sie eine Verbindung zu einer Lightsail-Windows-Instance unter Verwendung von Windows Remote-Desktop-Verbindung her

Mithilfe des Remotedesktopverbindungs-Clients ((RDC-Clients), der im Windows-Betriebssystem enthalten ist, können Sie eine Verbindung zu Ihrer Windows-Instance in Amazon Lightsail herstellen. RDC erfordert die Verwendung des Benutzernamens und Passworts des Administrators für die Windows-Instance. Hierbei kann es sich um das Standardpasswort handeln, das der Instance beim Erstellen zugewiesen wurde, oder um Ihr eigenes Passwort, wenn Sie das Standardpasswort geändert haben.

In diesem Thema werden die einzelnen Schritte zum Abrufen Ihres Standard-Administratorpassworts von der Lightsail-Konsole und zur Konfiguration von RDC für die Verbindung mit Ihrer Windows-Instance erläutert. Sie können auch über die Lightsail-Konsole unter Verwendung Ihres Browsers eine Verbindung zu Ihrer Instance herstellen. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Ihrer Windows-Instance mithilfe des webbasierten RDP-Clients.

Abrufen des Standard-Administratorpassworts für Ihre Windows-Instance

Führen Sie die folgenden Schritte aus, um das Standard-Administratorpasswort für Ihre Windows-Instance abzurufen, das für die Verbindung zu der Instance über RDC erforderlich ist.

> **Note**
>
> Wenn Sie das Standard-Administratorpasswort geändert haben, funktioniert das in der Lightsail-Konsole für Ihre Instance angezeigte Passwort nicht. Sie müssen sich Ihr Passwort merken. Ohne Ihr Administratorpasswort können Sie keine Verbindung zu Ihrer Instance über RDC herstellen.

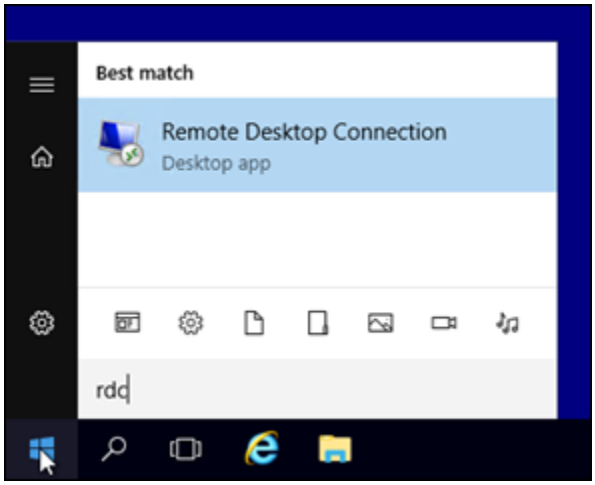
1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie die Windows Server-Instance aus, zu der Sie eine Verbindung herstellen möchten.
3. Wählen Sie auf der Registerkarte Connect (Verbinden) der Instance-Verwaltungsseite Show default password (Standardpasswort anzeigen) aus.
4. Markieren Sie das angezeigte Standardpasswort und kopieren Sie es durch Drücken von Ctl+C oder Cmd+C. Das Passwort ist jetzt auf der Zwischenablage.

   Fahren Sie mit dem nächsten Abschnitt dieses Handbuchs fort, um RDC zu konfigurieren, und fügen Sie das Passwort im Client ein.

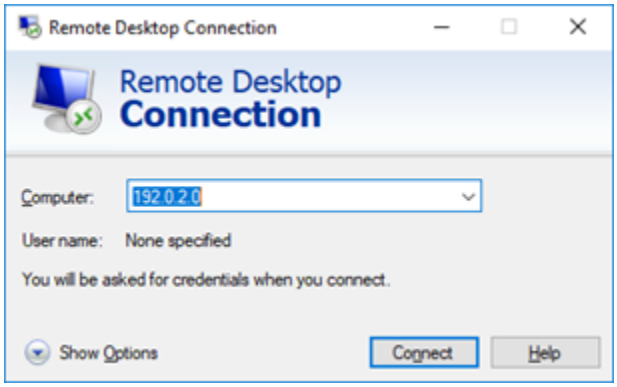
Konfigurieren von RDC und Verbinden mit Ihrer Windows-Instance

Führen Sie die folgenden Schritte aus, um RDC zu konfigurieren und eine Verbindung zu Ihrer Windows-Instance herzustellen.

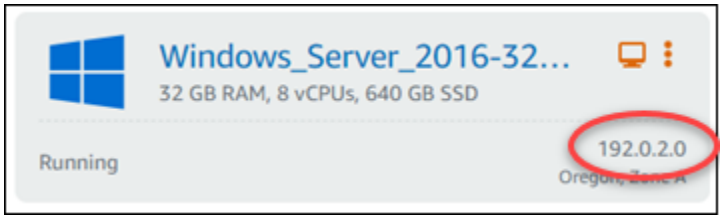
1. Öffnen Sie das Windows-Menü und suchen Sie nach `Remote Desktop Connection` oder `RDC`.
2. Wählen Sie Remote Desktop Connection (Remotedesktopverbindung) in den Suchergebnissen aus.



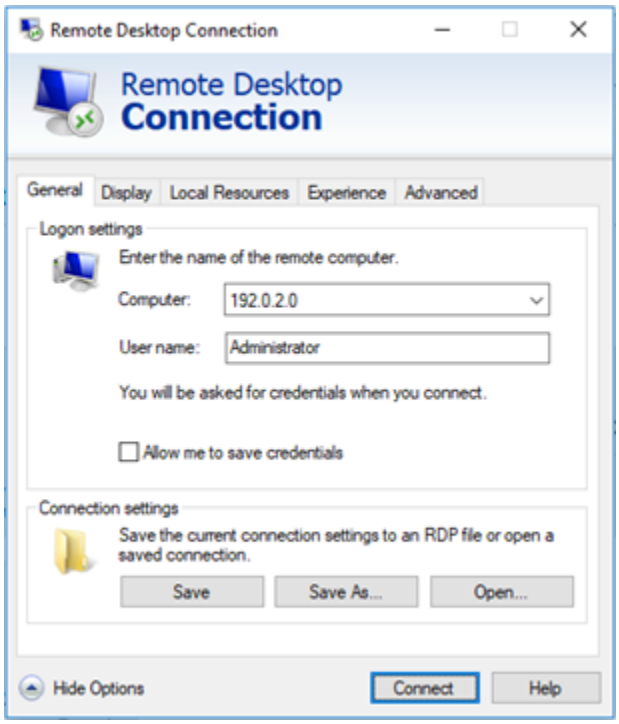
3. Geben Sie in das Textfeld Computer die öffentliche IP-Adresse Ihrer Windows-Instance ein.



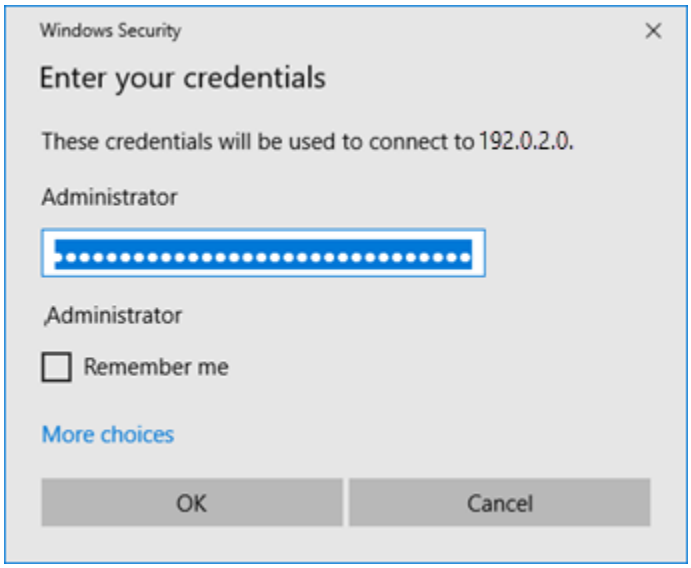
Die öffentliche IP wird in der Lightsail-Konsole neben Ihrer Instance angezeigt, wie im folgenden Beispiel dargestellt:



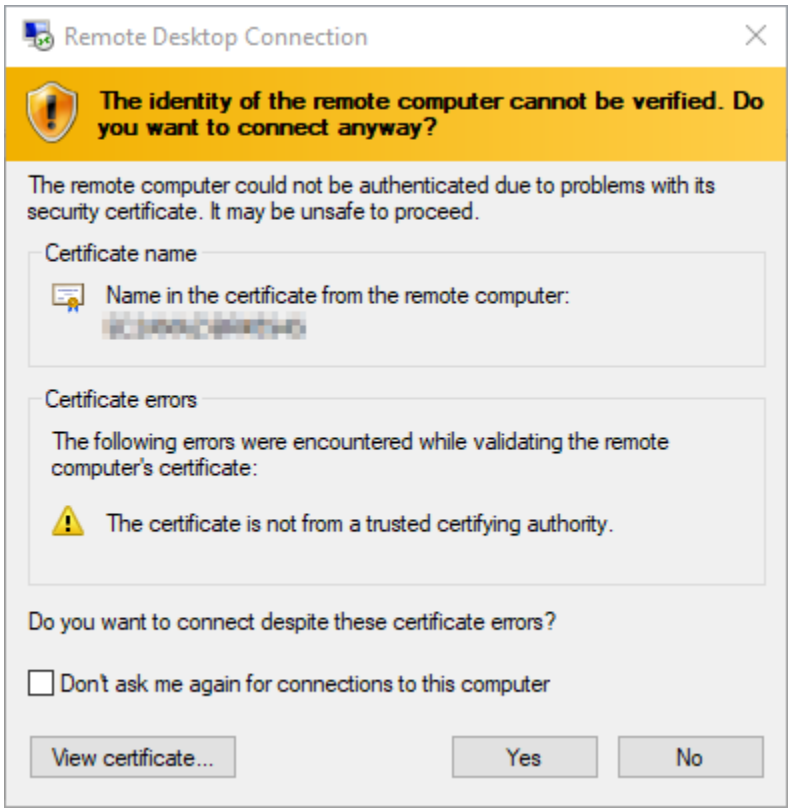
4. Wählen Sie Show Options (Optionen anzeigen) aus, um zusätzliche Verbindungsoptionen anzuzeigen.
5. In der Benutzername, geben Sie `Administrator` ein, was der Standard-Benutzername für alle Windows-Instances in Lightsail ist.



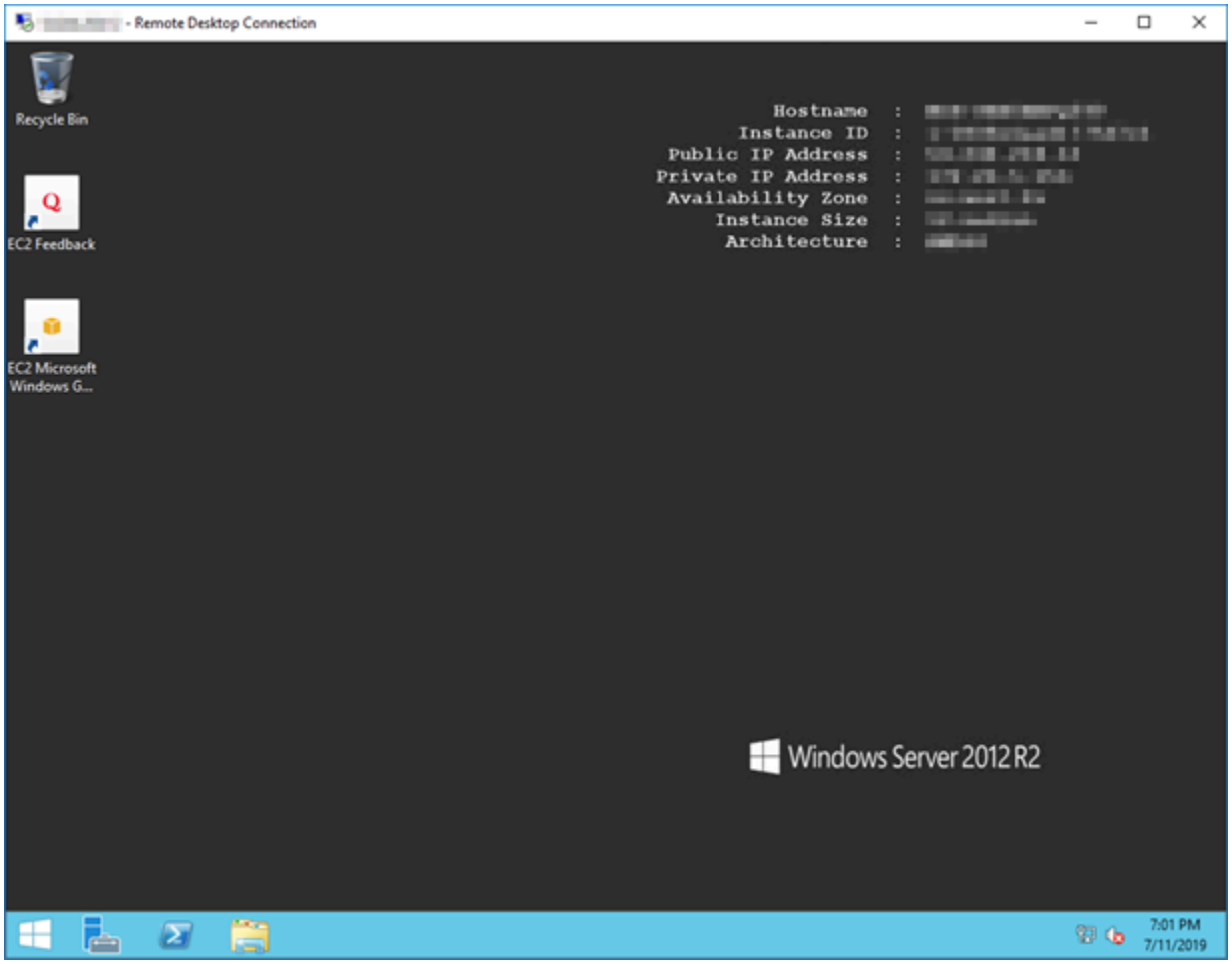
6. Wählen Sie Connect (Verbinden) aus.
7. Geben Sie in der angezeigten Eingabeaufforderung das Standard-Administratorpasswort ein oder fügen Sie das Passwort ein, das Sie zuvor aus der Lightsail-Konsole kopiert haben. Wählen Sie dann OK aus.



8. Wählen Sie in der angezeigten Eingabeaufforderung Yes (Ja) aus, um trotz Zertifikatsfehlern eine Verbindung zu der Windows-Instance herzustellen.



Nachdem Sie eine Verbindung zu der Instance hergestellt haben, sollte ein Bildschirm ähnlich dem folgenden Beispiel angezeigt werden:



Herstellen einer Verbindung mit einer Lightsail-Windows-Instance von macOS über Remote Desktop Connection

Mithilfe des Microsoft-Remote-Desktop-Clients können Sie von Ihrem macOS-Computer aus eine Verbindung zu Ihrer Windows-Instance herstellen. Microsoft Remote Desktop erfordert, dass Sie den Administratorbenutzernamen und das Administratorpasswort für Ihre Lightsail-Windows-Instance verwenden. Dies kann das Standardpasswort sein, das der Instance beim Erstellen zugewiesen wurde, oder Ihr eigenes Passwort, wenn Sie das Standardpasswort geändert haben.

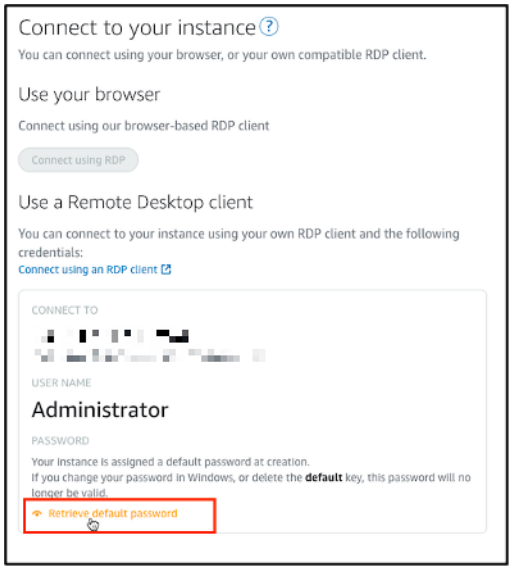
Dieses Thema führt Sie durch die Schritte zum Abrufen Ihres Standard-Administratorpassworts von der Lightsail-Konsole und zum Konfigurieren von Microsoft Remote Desktop für die Verbindung mit Ihrer Windows-Instance. Sie können sich auch von der Lightsail-Konsole aus über Ihren Browser mit Ihrer Instance verbinden. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Ihrer Windows-Instance mithilfe des Microsoft-Remote-Desktop-Clients.

Rufen Sie die erforderlichen Verbindungsinformationen für Ihre Windows-Instance ab

Sie benötigen die öffentliche IP-Adresse, den Benutzernamen und das Administratorkennwort, damit Ihre Windows-Instance über den Microsoft-Remote-Desktop-Client eine Verbindung herstellen kann.

Führen Sie das folgende Verfahren durch, um die erforderlichen Informationen abzurufen.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Instances.
3. Notieren Sie sich die öffentliche IP-Adresse der Instance, mit der Sie eine Verbindung herstellen möchten.
4. Wählen Sie den Namen der Instance aus, mit der Sie sich verbinden möchten.
5. Wählen Sie die Registerkarte Connect (Verbinden).
6. Wählen Sie Show default password (Standardpasswort anzeigen), um das Windows-Administratorkennwort für Ihre Instance zu erhalten.



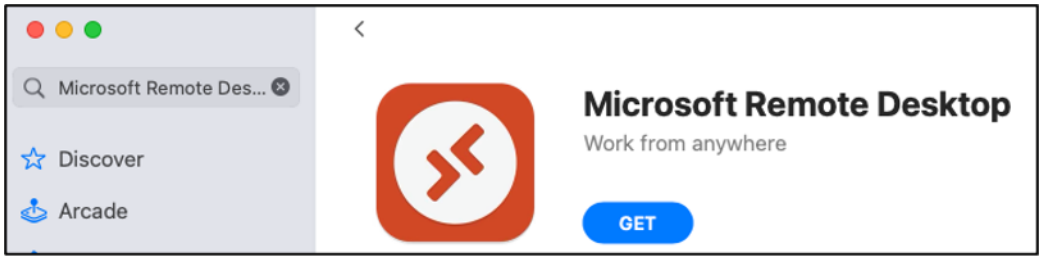
   In der Eingabeaufforderung wird das Standardadministratorkennwort für Ihre Windows-Instance angezeigt.

7. Kopieren Sie das Administrator-Passwort. Sie werden es verwenden, um sich später in diesem Leitfaden mit dem Microsoft-Remote-Desktop-Client bei Ihrer Instance anzumelden.

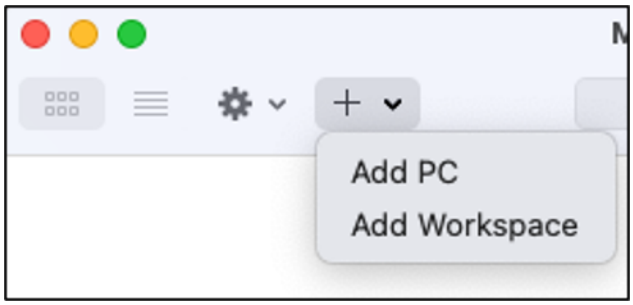
Konfigurieren Sie Microsoft Remote Desktop und stellen Sie eine Verbindung zu Ihrer Instance her

Vervollständigen Sie das folgende Verfahren, um den Microsoft-Remote-Desktop-Client auf Ihrem Mac zu installieren, und konfigurieren Sie ihn für die Verbindung mit Ihrer Instance.

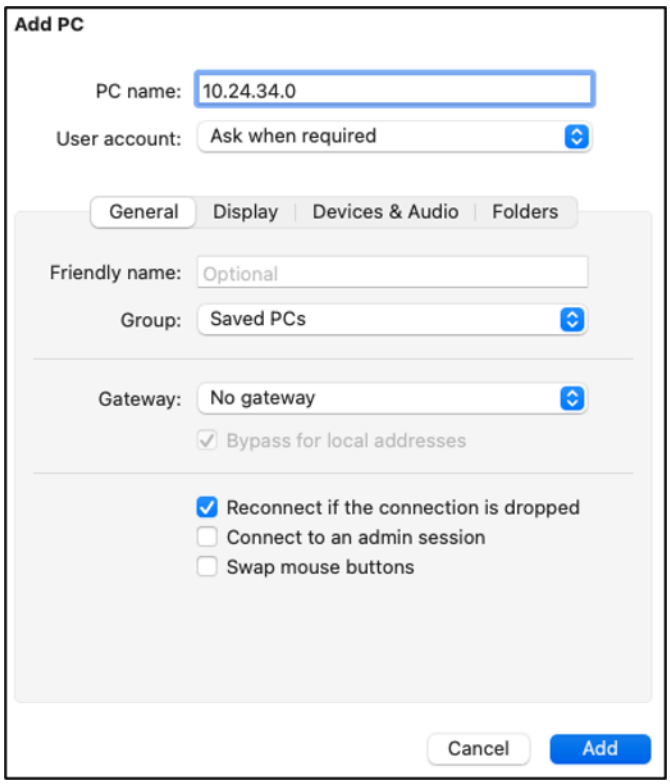
1. Öffnen Sie den App Store auf Ihrem Mac und suchen Sie nach Microsoft Remote Desktop.
2. Suchen Sie nach der Microsoft Remote Desktop-App in den Suchergebnissen und wählen Sie GET (ERHALTEN), um die Anwendung zu installieren.



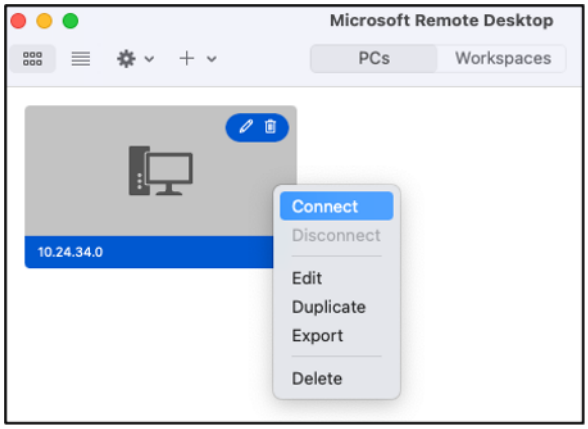
3. Öffnen Sie Microsoft Remote Desktop, nachdem die Installation abgeschlossen wurde.
4. Wählen Sie oben das Symbol plus (+) und wählen Sie PC hinzufügen.



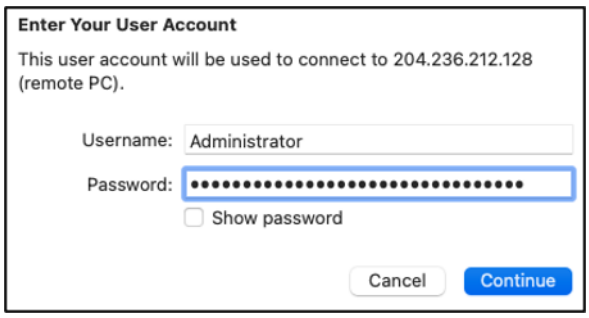
5. Fügen Sie im Textfeld PC name (PC-Name) die öffentliche IP-Adresse Ihrer Instance ein.
6. Wählen Sie Hinzufügen aus.



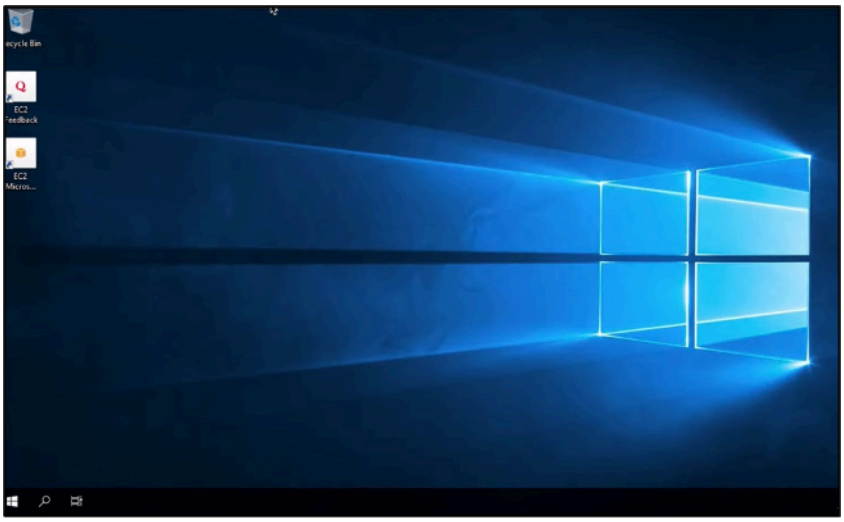
7. Rechtsklicken Sie auf das Symbol für Ihre Instance und wählen Sie Connect (Verbinden).



8. Geben Sie Administrator in das Benutzername:-Textfeld ein, und geben Sie das Standardadministratorkennwort ein, das Sie zuvor in diesem Leitfaden erhalten haben, in das Passwort-Textfeld ein.
9. Wählen Sie Continue (Fortfahren) aus, um eine Verbindung mit Ihrer Instance herzustellen.



Sie sind jetzt mit Ihrer Lightsail-Windows-Instance verbunden.



Erstellen eines Snapshots Ihrer Linux-/Unix-basierten Lightsail-Instance

Sie können Snapshots Ihrer Linux-/Unix-basierten Lightsail-Instances erstellen. Ein Instance-Snapshot ist eine Kopie des Systemdatenträgers und stimmt mit der Konfiguration des ursprünglichen Systems überein (Speicher, CPU, Festplattengröße und Datenübertragungsgeschwindigkeit). Wenn Sie Ihrer Instance Blockspeicherdatenträger angefügt haben, kopiert Lightsail diese zusätzlichen Datenträger als Teil Ihres Snapshots. Weitere Informationen finden Sie unter Snapshots.

> **Note**
>
> Die Schritte zum Erstellen eines Snapshots einer Windows Server-basierten Lightsail-Instance unterscheiden sich. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Windows-Server-Instance.

Sie müssen bereits eine Instance in Lightsail haben, um einen Snapshot erstellen zu können. Nachdem Sie eine Instance zur Verfügung gestellt haben, führen Sie die folgenden Schritte aus, um einen Snapshot zu erstellen:

1. Wählen Sie auf der Startseite von Lightsail den Namen der Windows Server-Instance, für die Sie einen Snapshot erstellen möchten.
2. Wählen Sie die Registerkarte Snapshots aus.
3. Wählen Sie im Abschnitt Manual snapshots (Manuelle Snapshots) der Seite Create snapshot (Snapshot erstellen) und geben Sie dann einen Namen für Ihren Snapshot ein.

   Ressourcennamen:

   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.
4. Wählen Sie Erstellen aus.

   Sie können den soeben erstellten Snapshot mit dem Status Snapshotting... anzeigen.

   Nachdem der Snapshot fertig ist, können Sie eine andere Instance aus dem Snapshot erstellen. Beispielsweise können Sie ein größeres Paket als bisher wählen.

> **Important**
>
> Wenn Sie eine neue Instance aus einem Snapshot erstellen, lässt Lightsail, Sie ein Instance-Paket derselben Größe oder größer erstellen. Wir unterstützen derzeit keine Möglichkeit, eine kleinere Instance-Größe aus einem Snapshot zu erstellen. Die kleineren Optionen werden ausgegraut dargestellt, wenn Sie eine neue Instance aus einem Snapshot erstellen.

Um eine größere Instance aus einem Snapshot zu erstellen, verwenden Sie auf der Lightsail-Konsole den CLI-Befehl create-instances-from-snapshot oder die API-Operation CreateInstancesFromSnapshot. Weitere Informationen finden Sie unter Erstellen einer Instance aus einem Snapshot.

Weitere Informationen zu Lightsail-Paketen finden Sie unter Lightsail-Preise.

Themen

Herstellen einer Verbindung mit einer Linux- oder Unix-Instance in Amazon EC2, die aus einem Amazon Lightsail-Snapshot erstellt wurde

Nachdem eine Linux- oder Unix-Instance in Amazon Elastic Compute Cloud (Amazon EC2) aus einem Amazon Lightsail-Snapshot erstellt wurde, können Sie sich über SSH mit der Instance verbinden, ähnlich wie Sie eine Verbindung mit der Lightsail-Quell-Instance hergestellt haben. Um sich bei Ihrer Instance zu authentifizieren, verwenden Sie entweder das standardmäßige Lightsail-Schlüsselpaar für die der Quell AWS-Region-Instance oder Ihr eigenes Schlüsselpaar. Dieses Handbuch zeigt Ihnen, wie Sie sich mit PuTTY mit Ihrer Linux- oder Unix-Instance in EC2 verbinden.

> **Note**
>
> Weitere Informationen zum Herstellen einer Verbindung mit einer Windows Server-Instance finden Sie unter Herstellen einer Verbindung mit einer Amazon EC2 Windows Server-Instance, die aus einem Lightsail-Snapshot erstellt wurde.

Inhalt

- Nächste Schritte

Abrufen des Schlüssels für Ihre Instance

Holen Sie sich den richtigen Schlüssel, der für die Verbindung zu Ihrer neuen Amazon-EC2-Instance erforderlich ist. Der benötigte Schlüssel hängt davon ab, wie Sie eine Verbindung mit der Lightsail-Quell-Instance hergestellt haben. Sie können sich mit einer der folgenden Methoden mit der Quell-Lightsail-Instance verbinden:

- Verwenden des standardmäßigen Lightsail-Schlüsselpaars für die Region der Quell-Instance – Laden Sie den privaten Standardschlüssel von der Registerkarte SSH-Schlüssel auf der Lightsail-Kontoseite herunter. Weitere Informationen zu den standardmäßigen Lightsail-Schlüsseln finden Sie unter SSH-Schlüsselpaare.

  > **Note**
  >
  > Nachdem Sie eine Verbindung zu Ihrer EC2-Instance hergestellt haben, empfehlen wir, den standardmäßigen Lightsail-Schlüssel aus der Instance zu entfernen und durch Ihr eigenes Schlüsselpaar zu ersetzen. Weitere Informationen finden Sie unter Sichern Ihrer Linux- oder Unix-Instance in Amazon EC2, die aus einem Lightsail-Snapshot erstellt wurde.

- Verwendung Ihres eigenen Schlüsselpaars – Suchen Sie den privaten Schlüssel und verbinden Sie sich mit ihm mit Ihrer Amazon EC2-Instance. Lightsail speichert Ihren privaten Schlüssel nicht, wenn Sie Ihr eigenes Schlüsselpaar verwenden. Wenn Sie Ihren privaten Schlüssel verloren haben, können Sie sich nicht mit Ihrer Amazon-EC2-Instance verbinden.

Abrufen der öffentlichen DNS-Adresse für Ihre Instance

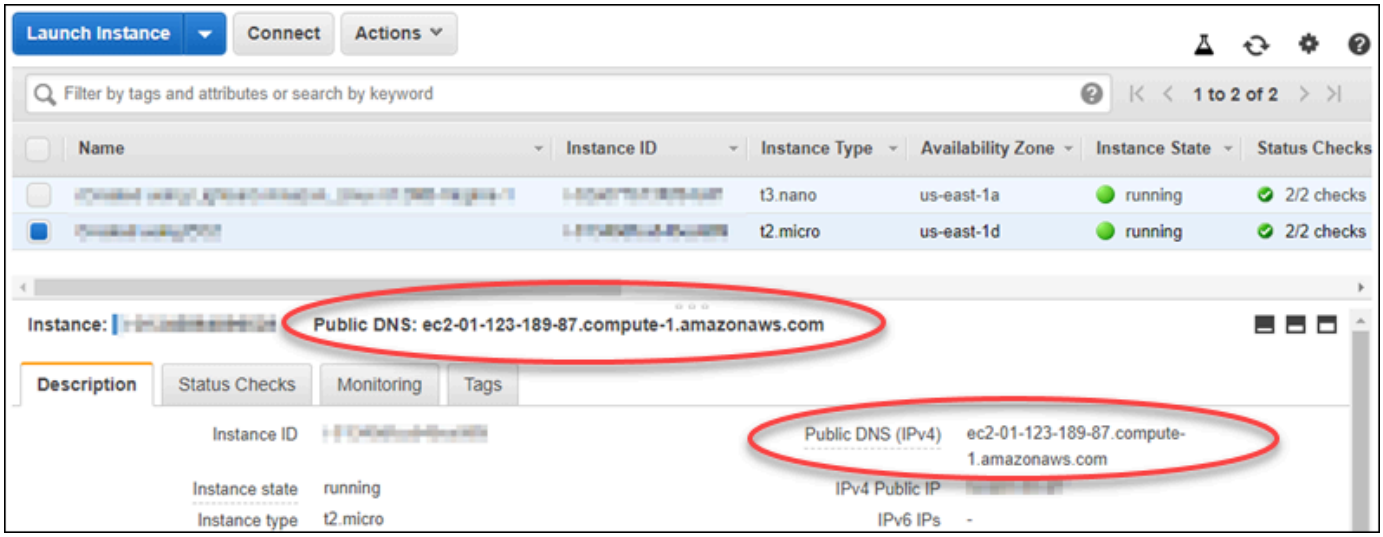
Rufen Sie die öffentliche DNS-Adresse für Ihre Amazon-EC2-Instance ab, sodass Sie sie bei der Konfiguration eines SSH-Clients, wie beispielsweise PuTTY, verwenden können, um eine Verbindung zu Ihrer Instance herzustellen.

So rufen Sie den die öffentlichen DNS-Adresse für Ihre Instance ab

1. Melden Sie sich bei der Amazon-EC2-Konsole an.
2. Wählen Sie im linken Navigationsbereich Instances aus.

3. Wählen Sie die laufende Linux- oder Unix-Instance aus, mit der Sie eine Verbindung herstellen möchten.
4. Suchen Sie im unteren Bereich die Public DNS (Öffentliche DNS)-Adresse für Ihre Instance.

   Dies ist die Adresse, die Sie bei der Konfiguration eines SSH-Clients verwenden werden, um eine Verbindung zu Ihrer Instance herzustellen. Fahren Sie mit dem Abschnitt Herunterladen und Installieren von PuTTY in diesem Handbuch fort, um zu erfahren, wie Sie den PuTTY SSH-Client herunterladen und installieren.



Herunterladen und Installieren von PuTTY

PuTTY ist ein kostenloser SSH-Client für Windows. Für weitere Informationen über PuTTY finden Sie in "PuTTY: a free SSH and Telnet client". Diese Website beschreibt auch die Einschränkungen in Ländern, in denen die Verschlüsselung nicht erlaubt ist. Wenn Sie bereits über PuTTY verfügen, können Sie mit dem folgenden Abschnitt Konfigurieren des Schlüssels mit PuTTYgen in diesem Handbuch fortfahren.

Laden Sie das PuTTY-Installationsprogramm oder die ausführbare Datei herunter. Wir empfehlen die Verwendung der neuesten Version. Informationen darüber, welchen Download Sie auswählen sollten, finden Sie in der PuTTY-Dokumentation.

Fahren Sie mit dem Abschnitt Konfigurieren des Schlüssels mit PuTTYgen in diesem Handbuch fort, um den Schlüssel mit PuTTYgen zu konfigurieren.

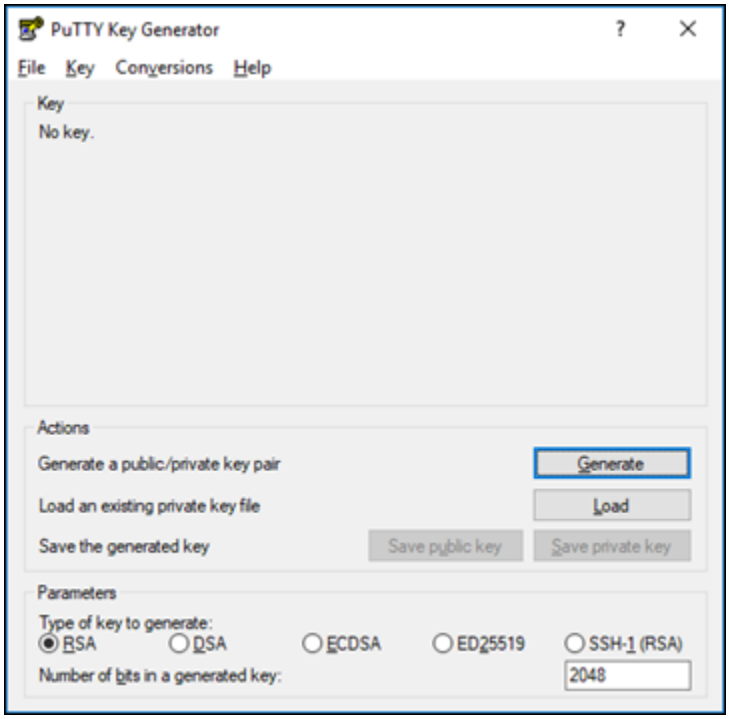
Konfigurieren des Schlüssels mit PuTTYgen

PuTTYgen generiert Paare von öffentlichen und privaten Schlüsseln, die mit PuTTY verwendet werden können. Dieser Schritt ist erforderlich, um den von PuTTY akzeptierten Schlüsseldateityp (PPK) zu verwenden.

So konfigurieren Sie den Schlüssel mit PuTTYgen

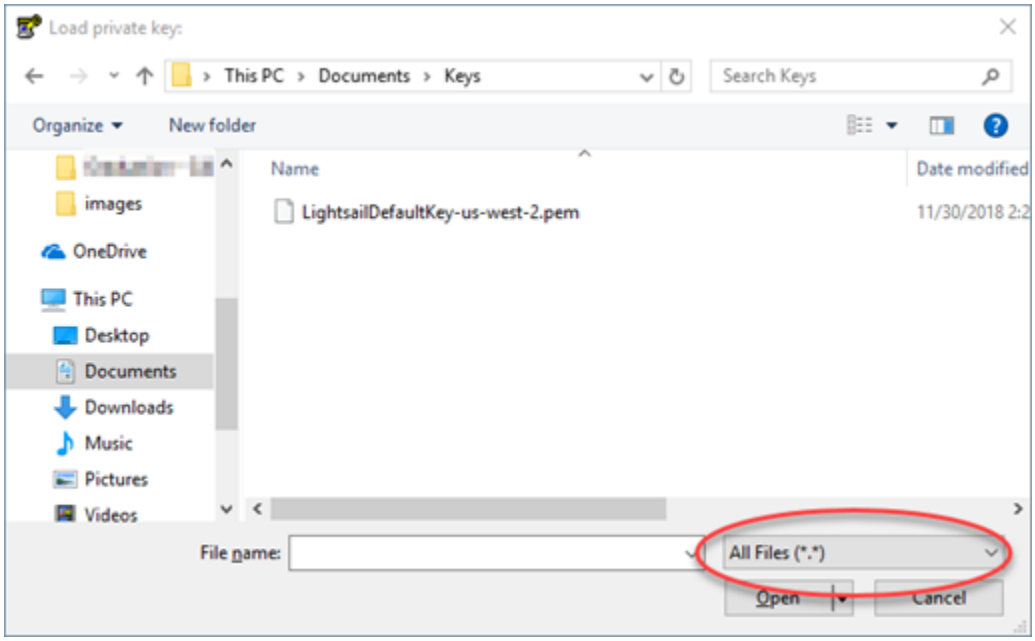
1. Starten Sie PuTTYgen.

   Wählen Sie beispielsweise das Windows-Startmenü aus. Wählen Sie dann Alle Programme, PuTTY und PuTTYgen aus.

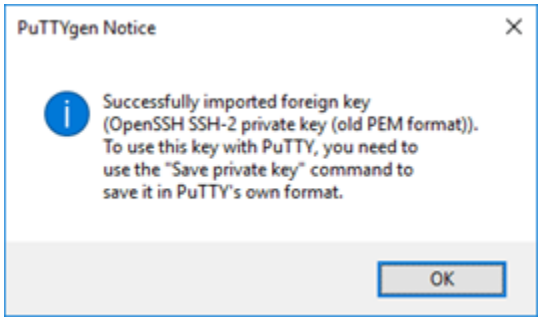


2. Wählen Sie Laden aus.

   PuTTYgen zeigt standardmäßig nur Dateien mit der Erweiterung PPK an. Damit Sie die PEM-Datei finden, wählen Sie die Option zur Anzeige aller Dateitypen.

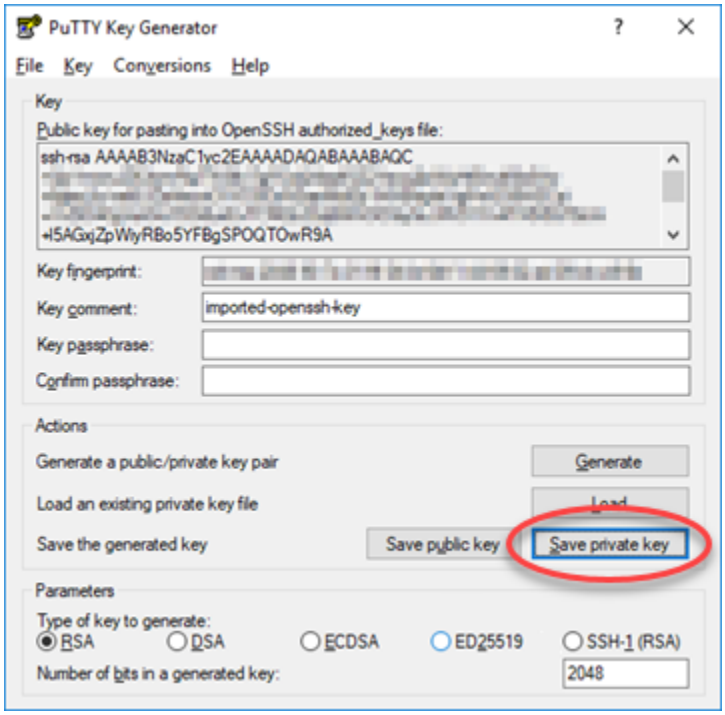


3. Wählen Sie die standardmäßige Lightsail-Schlüsseldatei (.PEM), die Sie zuvor in diesem Handbuch heruntergeladen haben, und wählen Sie dann Öffnen aus.
4. Nachdem PuTTYgen bestätigt hat, dass Sie den Schlüssel erfolgreich importiert haben, wählen Sie OK aus.



5. Wählen Sie Save private key (Privaten Schlüssel speichern) und bestätigen Sie, dass Sie ihn nicht mit einer Passphrase speichern möchten.

   Wenn Sie eine Passphrase als zusätzliche Sicherheitsmaßnahme erstellen wollen, denken Sie daran, dass Sie sie jedes Mal eingeben müssen, wenn Sie eine Verbindung mit Ihrer Instance mithilfe von PuTTY herstellen.



6. Geben Sie einen Namen und einen Speicherort für Ihren privaten Schlüssel an, und wählen Sie anschließend Save (Speichern).

   PuTTYgen speichert Ihre neue Schlüsseldatei als PPK-Dateityp.

7. Schließen Sie PuTTygen.

   Fahren Sie mit dem Abschnitt Konfigurieren von PuTTY, um eine Verbindung zu Ihrer Instance herzustellen in diesem Handbuch fort, um die neue PPK-Datei zu verwenden, die Sie zur Konfiguration von PuTTY und zur Verbindung mit Ihrer Linux- oder Unix-Instance in Amazon EC2 generiert haben.

Konfigurieren von PuTTY, um eine Verbindung zu Ihrer Instance herzustellen

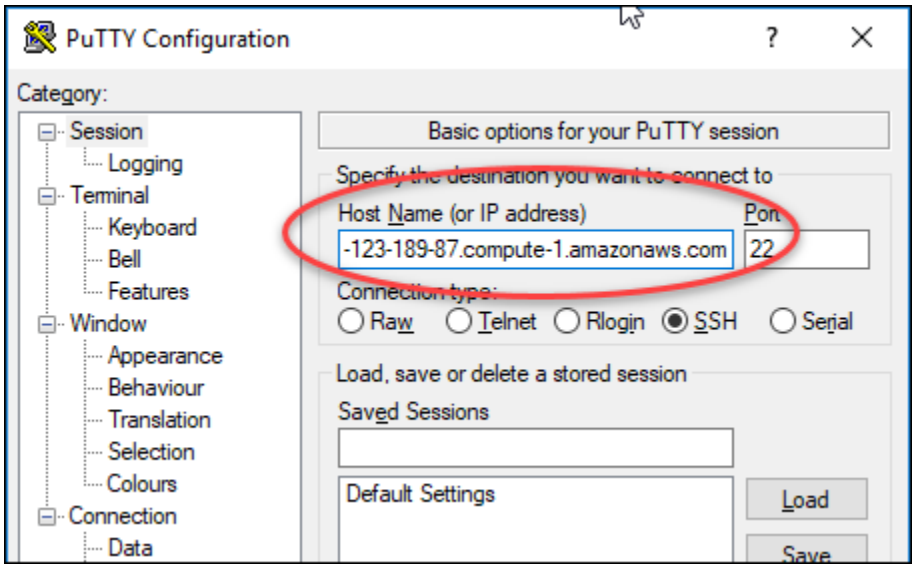
Nachdem alle Voraussetzungen erfüllt sind, konfigurieren Sie PuTTY, um sich mit Ihrer Linux- oder Unix-Instance über SSH zu verbinden.

So konfigurieren Sie PuTTY für die Verbindung mit Ihrer Linux- oder Unix-Instance

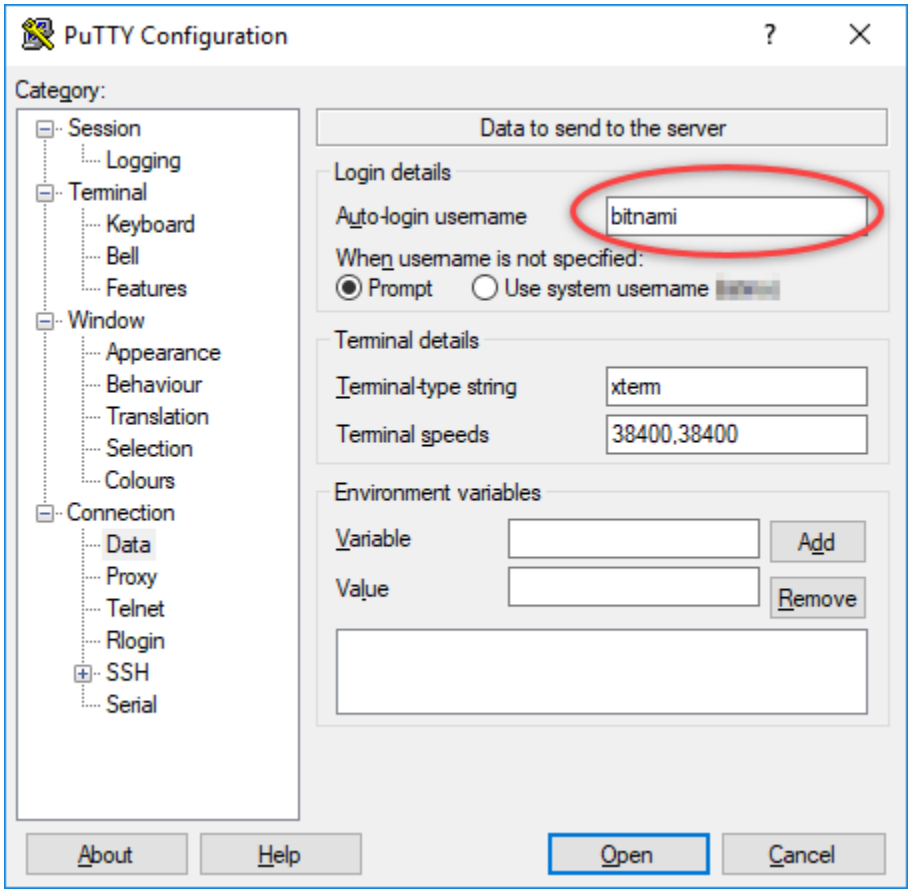
1. Öffnen Sie PuTTY.

   Wählen Sie beispielsweise das Windows-Startmenü aus. Wählen Sie dann Alle Programme, PuTTY und PuTTY aus.

2. Geben Sie im Textfeld Hostname die öffentliche DNS-Adresse für Ihre Instance ein, die Sie zuvor in diesem Handbuch über die Amazon-EC2-Konsole erhalten haben.



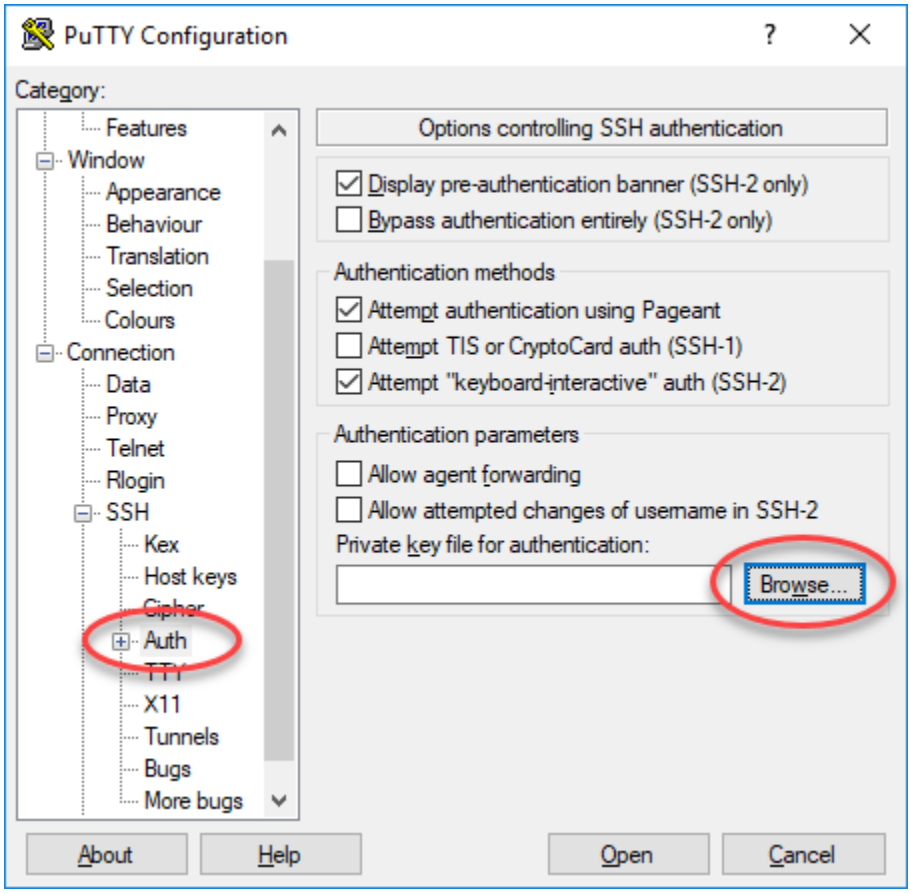
3. Wählen Sie im linken Navigationsbereich unter dem Abschnitt Connection (Verbindung) die Option Data (Daten) aus.
4. Geben Sie im Textfeld Auto-login username (Auto-Login-Benutzername) einen Benutzernamen ein, der bei der Anmeldung an der Instance verwendet werden soll.



Geben Sie je nach Vorlage der Lightsail-Quell-Instance einen der folgenden Standardbenutzernamen ein:

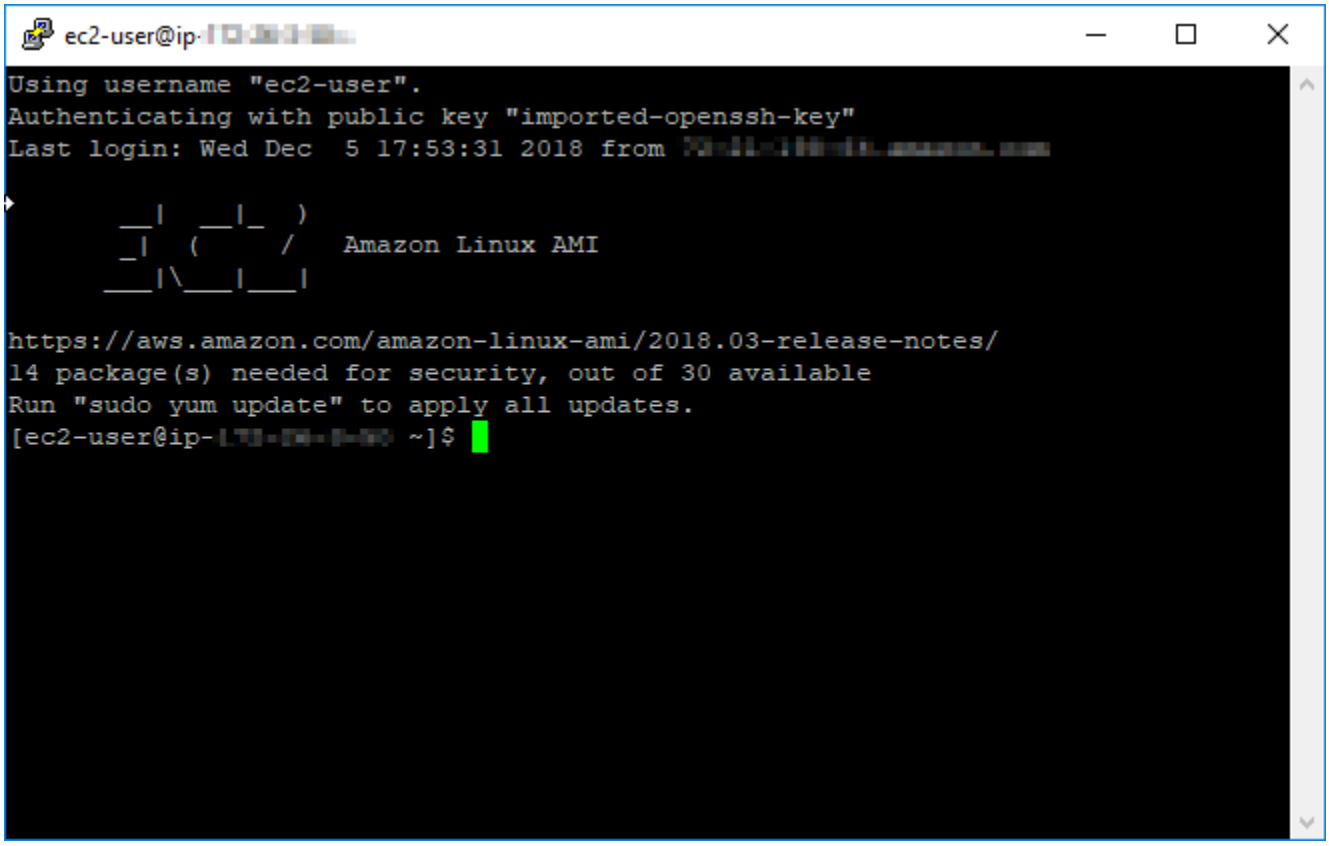
- AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, FreeBSD und openSUSE-Instances: `ec2-user`
- CentOS-7-Instances: `centos`
- Debian-Instances: `admin`
- Ubuntu-Instances: `ubuntu`
- Bitnami-Instances: `bitnami`
- Plesk-Instances: `ubuntu`
- cPanel & WHM-Instances: `centos`

5. Erweitern Sie im linken Navigationsbereich unter dem Abschnitt Connection (Verbindung) die Option SSH und wählen Sie dann Auth aus.
6. Wählen Sie Browse (Durchsuchen), um zur PPK-Datei zu gelangen, die Sie im vorherigen Schritt erstellt haben, und klicken Sie dann auf Open (Öffnen).



7. Klicken Sie erneut auf Open (Öffnen), um sich mit Ihrer Instance zu verbinden und klicken Sie dann auf Yes (Ja), um dieser Verbindung in Zukunft zu vertrauen.

   Sie sollten eine Seite ähnlich der folgenden sehen, wenn Sie sich erfolgreich mit Ihrer Instance verbunden haben:



Nächste Schritte

Ihre neue Linux- oder Unix-Instance in Amazon EC2 enthält Restschlüssel aus dem Lightsail-Service, wenn Sie Amazon EC2 verwenden, um neue Instances aus Ihren exportierten Snapshots zu erstellen. Wir empfehlen, diese Schlüssel zu entfernen, um die Sicherheit für Ihre neue Amazon-EC2-Instance zu erhöhen. Weitere Informationen finden Sie unter Sichern Ihrer Linux- oder Unix-Instance in Amazon EC2, die aus einem Lightsail-Snapshot erstellt wurde.

Verbinden mit einer Windows-Server-Instance in Amazon EC2, die aus einem Lightsail-Snapshot erstellt wurde

Nachdem Ihre neue Windows Server-Instance in Amazon Elastic Compute Cloud (Amazon EC2) erstellt wurde, können Sie sich mit dem Remote Desktop Protocol (RDP) mit ihr verbinden. Dies ist ähnlich wie bei der Verbindung zur Amazon Lightsail-Quell-Instance. Stellen Sie mit dem Standard-Lightsail-Schlüsselpaar für die AWS-Region der Quell-Instance eine Verbindung zu Ihrer EC2-Instance her. In dieser Anleitung erfahren Sie, wie Sie mit Microsoft Remotedesktopverbindung eine Verbindung zu Ihrer Windows Server-Instance herstellen.

> **Note**
>
> Weitere Informationen zur Verbindung mit einer Linux- oder Unix-Instance finden Sie unter Verbindung mit einer Linux- oder Unix-Instance in Amazon EC2, die aus einem Lightsail-Snapshot erstellt wurde.

Inhalt

Abrufen des Schlüssels für Ihre Instance

Ihre Windows-Server-Instance in Amazon EC2 verwendet das Standard-Lightsail-Schlüsselpaar für die Region der Quell-Instance, um das Standard-Administratorpasswort abzurufen.

Laden Sie den standardmäßigen privaten Schlüssel von der Registerkarte SSH keys (SSH-Schlüssel) auf der Lightsail-Kontoseite herunter. Weitere Informationen zum Verwenden des Standard-Lightsail-SSH-Schlüssels finden Sie unter SSH-Schlüsselpaare.

> **Note**
>
> Nachdem Sie sich mit Ihrer EC2-Instance verbunden haben, empfehlen wir, das Administratorpasswort für Ihre Windows-Server-Instance in Amazon EC2 zu ändern. Dies entfernt die Zuordnung zwischen dem Standard-Lightsail-Schlüsselpaar und Ihrer Windows-Server-Instance in Amazon EC2. Weitere Informationen finden Sie unter Sichern einer Instance von Amazon EC2 Windows Server, die aus einem Lightsail-Snapshot erstellt wurde.

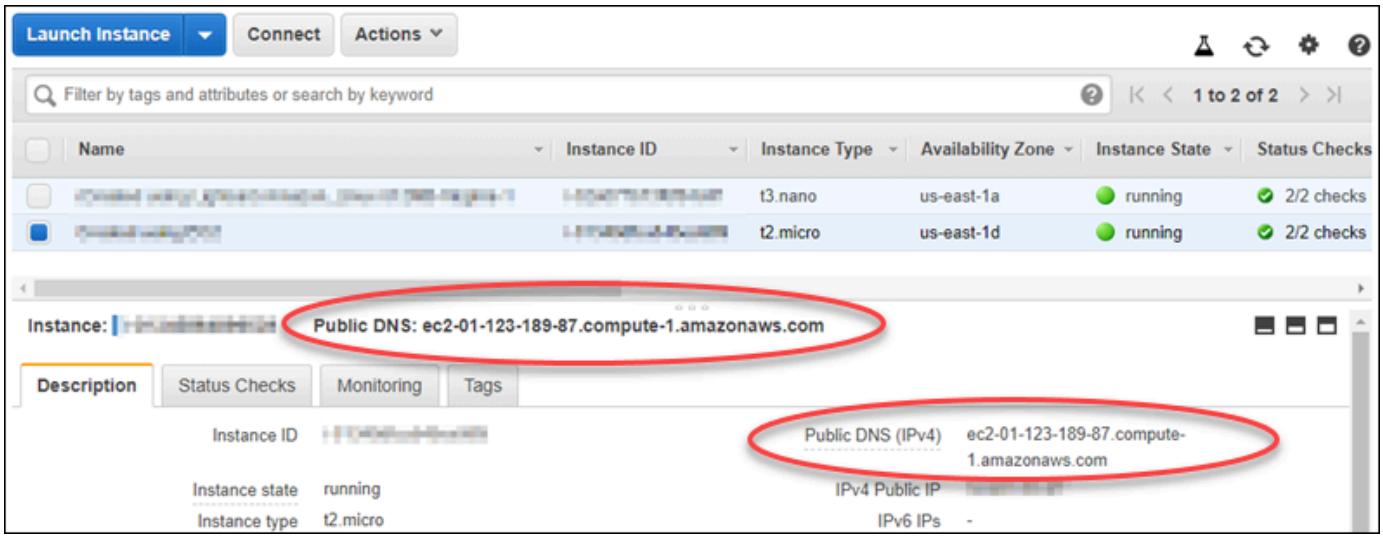
Abrufen der öffentlichen DNS-Adresse für Ihre Instance

Rufen Sie die öffentliche DNS-Adresse für Ihre Amazon-EC2-Instance ab, sodass Sie sie bei der Konfiguration eines RDP-Clients, wie beispielsweise Microsoft-Remotedektopverbindung, verwenden können, um eine Verbindung zu Ihrer Instance herzustellen.

So rufen Sie den die öffentlichen DNS-Adresse für Ihre Instance ab

1. Melden Sie sich bei der Amazon-EC2-Konsole an.
2. Wählen Sie im linken Navigationsbereich Instances aus.
3. Wählen Sie die laufende Windows Server-Instance, mit der Sie eine Verbindung herstellen möchten.
4. Suchen Sie im unteren Bereich die Public DNS (Öffentliche DNS)-Adresse für Ihre Instance.

   Dies ist die Adresse, die Sie bei der Konfiguration eines RDP-Clients verwenden werden, um eine Verbindung zu Ihrer Instance herzustellen. Fahren Sie mit dem Abschnitt Abrufen des Passworts für Ihre Windows-Server-Instance in diesem Handbuch fort, um zu erfahren, wie Sie das Standard-Administratorpasswort für Ihre Windows-Server-Instance in Amazon EC2 abrufen.

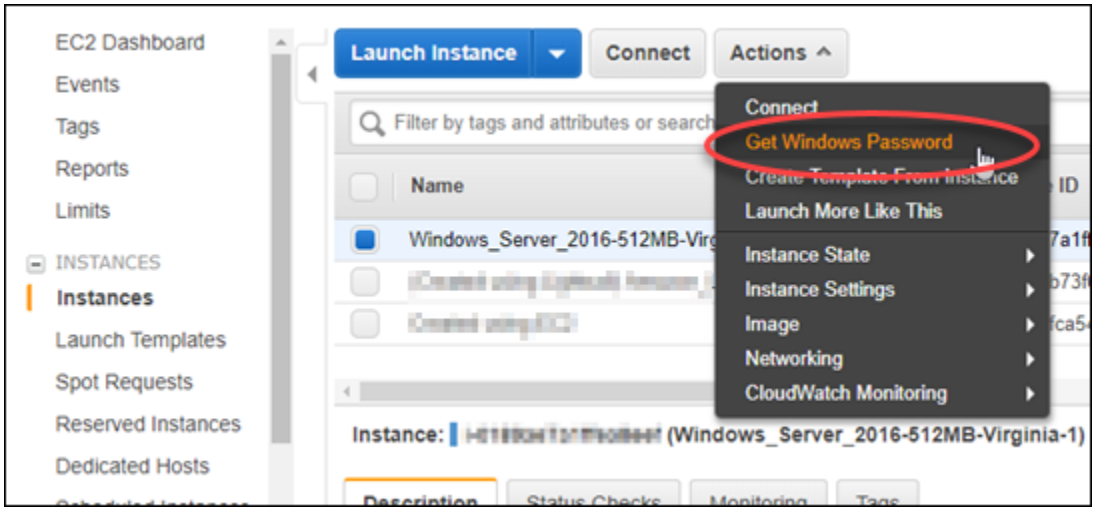


Abrufen des Passworts für Ihre Windows Server-Instance

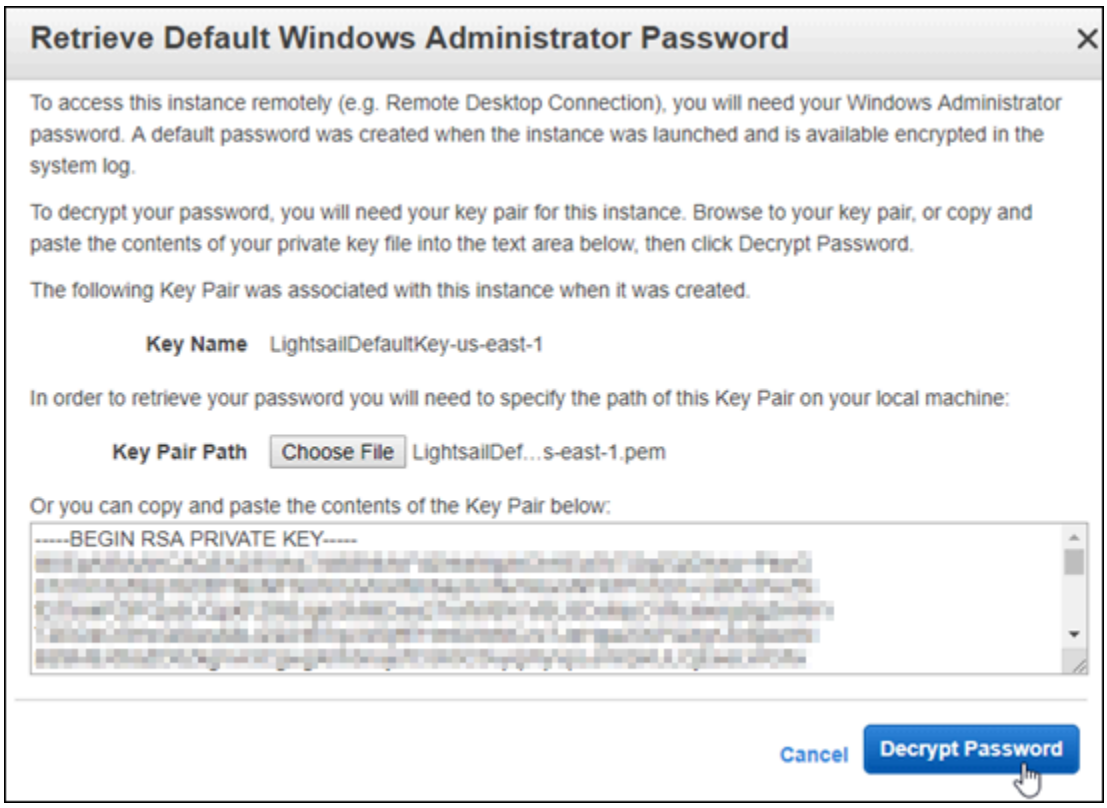
Rufen Sie das Passwort für Ihre Windows-Server-Instance über die Amazon-EC2-Konsole ab. Sie benötigen dieses Passwort, um sich bei Ihrer Windows Server-Instance anzumelden, wenn Sie sich über RDP mit ihr verbinden.

So erhalten Sie das Passwort für Ihre Windows Server-Instance

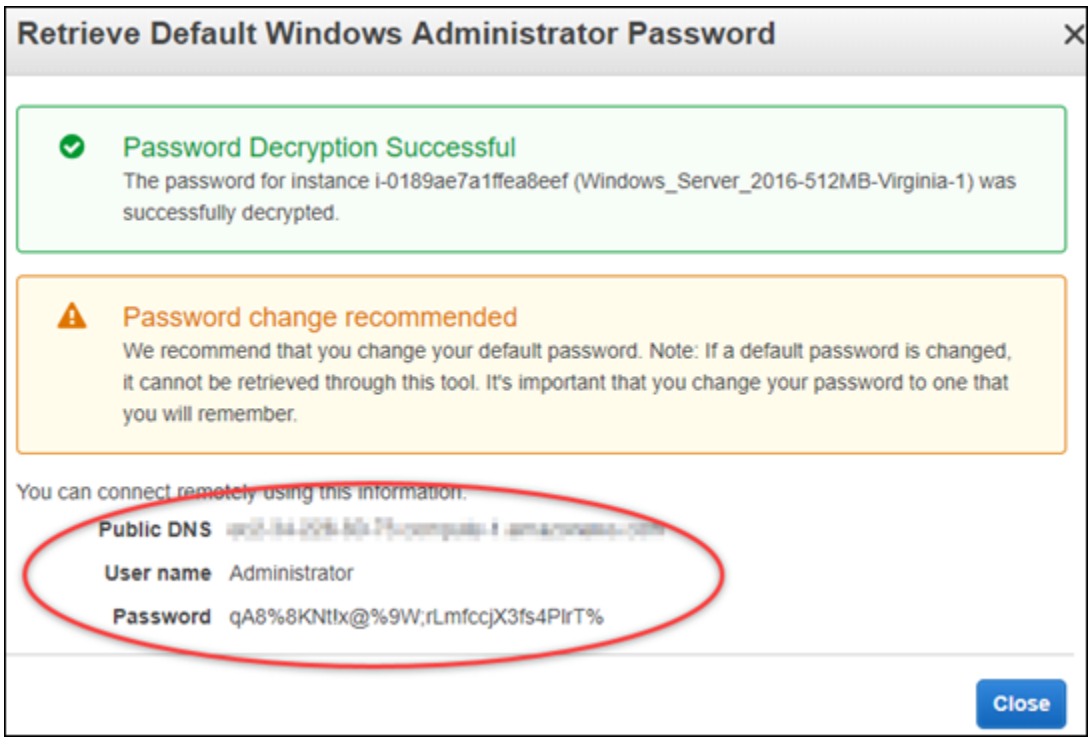
1. Melden Sie sich bei der Amazon-EC2-Konsole an.
2. Wählen Sie im linken Navigationsbereich Instances aus.
3. Wählen Sie die Windows Server-Instance, mit der Sie eine Verbindung herstellen möchten.
4. Wählen Sie Actions (Aktionen) und dann Get Windows Password (Windows-Passwort abrufen) aus.



5. Wählen Sie an der Eingabeaufforderung Browse (Durchsuchen) aus und öffnen Sie die standardmäßige private Schlüsseldatei, die Sie zuvor von Lightsail heruntergeladen haben.
6. Klicken Sie auf Decrypt Password.



Das Passwort wird auf dem Bildschirm angezeigt, ebenso wie der öffentliche DNS- und Benutzername. Kopieren Sie das Passwort in die Zwischenablage, damit Sie es im folgenden Abschnitt Konfigurieren einer Remotedesktopverbindung für die Verbindung zu Ihrer Windows Server-Instance in diesem Handbuch verwenden können. Markieren Sie das Password und drücken Sie Ctrl+C (Strg+C), wenn Sie Windows verwenden, oder Cmd+C, wenn Sie macOS verwenden.



Fahren Sie mit dem Abschnitt Konfigurieren einer Remotedesktopverbindung für die Verbindung zu Ihrer Windows-Server-Instance in diesem Handbuch fort, um zu erfahren, wie Sie eine Remotedesktopverbindung für die Verbindung mit Ihrer Windows-Server-Instance unter Amazon EC2 konfigurieren.

Konfigurieren der Remotedesktopverbindung für eine Verbindung zu Ihrer Windows Server-Instance

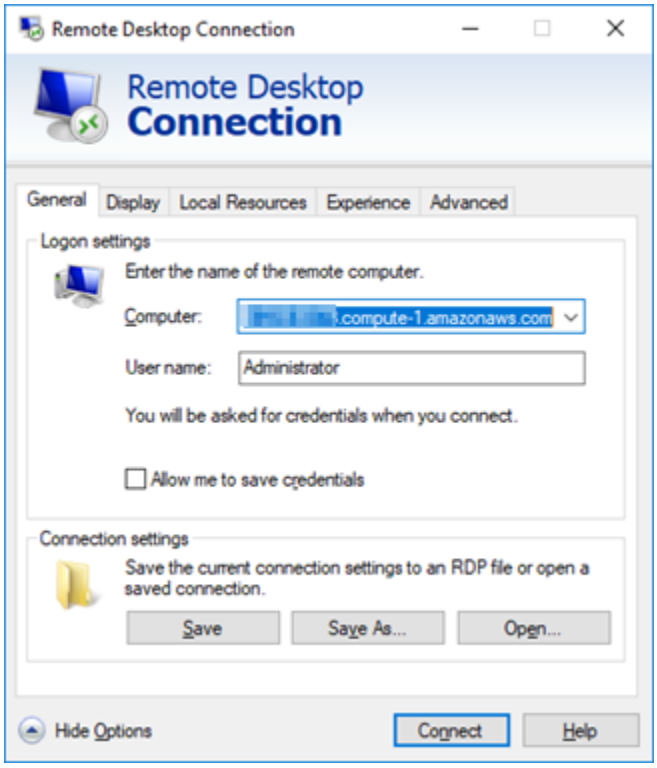
Remotedesktopverbindung ist ein RDP-Client, der in den meisten Windows-Betriebssystemen vorinstalliert ist. Verwenden Sie es, um eine grafische Verbindung zu Ihrer Windows-Server-Instance unter Amazon EC2 herzustellen.

So konfigurieren Sie die Remotedesktopverbindung für die Verbindung mit Ihrer Windows Server-Instance

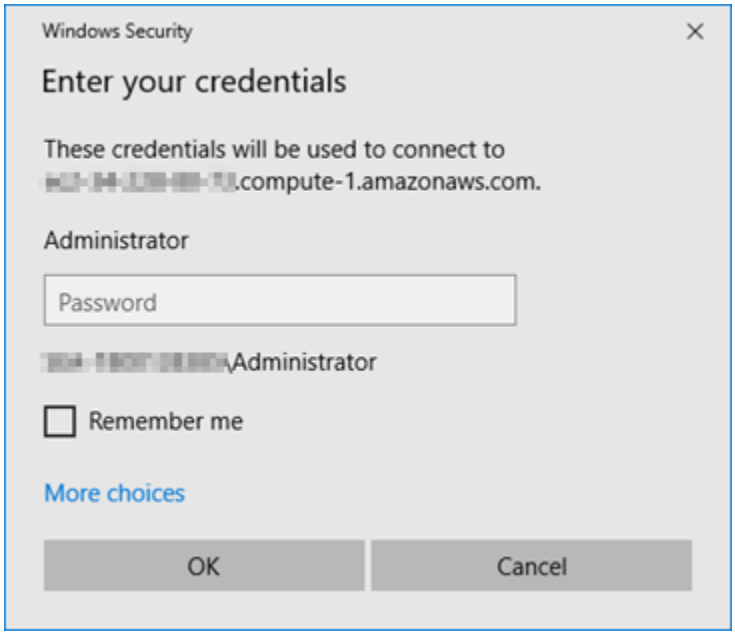
1. Öffnen Sie die Remotedesktopverbindung.

   Wählen Sie beispielsweise das Windows-Startmenü aus und suchen Sie dann nach Remotedesktopverbindung.
2. Geben Sie im Textfeld Computer die öffentliche DNS-Adresse für Ihre Windows-Server-Instance in Amazon EC2 ein, die Sie zuvor in diesem Handbuch erhalten haben.

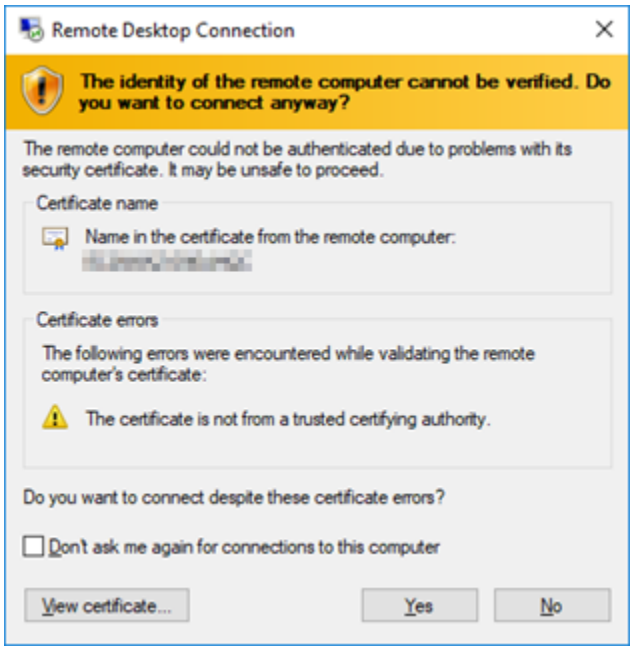
3. Wählen Sie Optionen anzeigen aus, um weitere Optionen anzuzeigen.
4. Geben Sie `Administrator` in das Textfeld Benutzername ein.



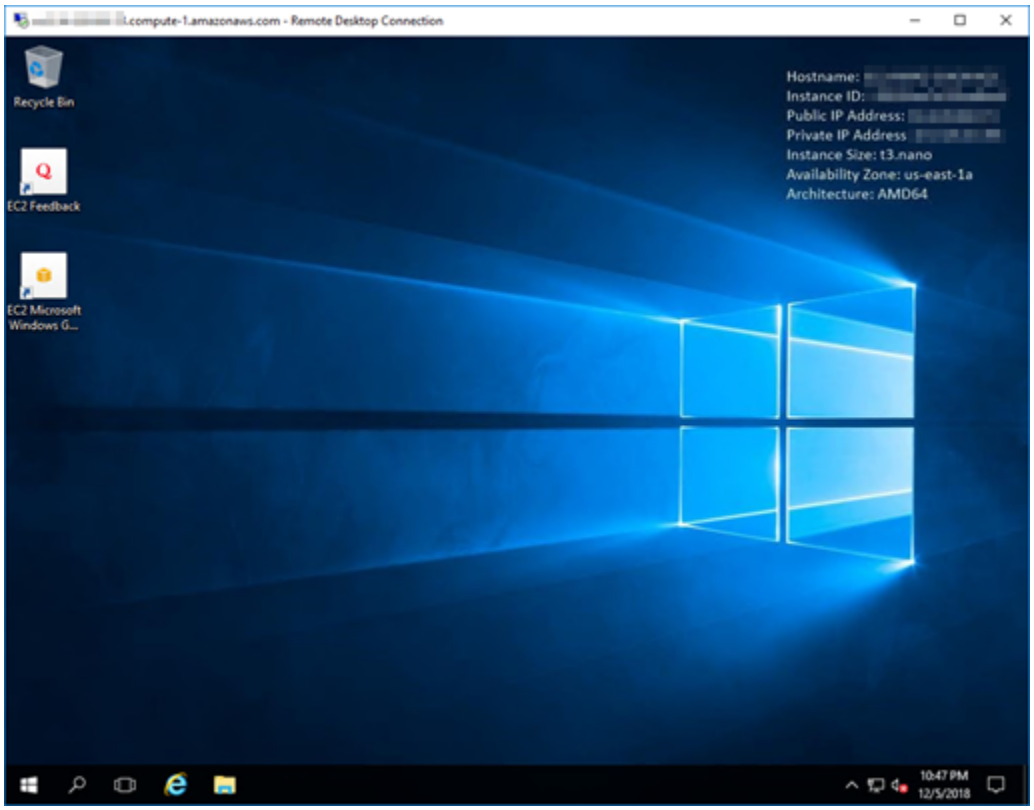
5. Wählen Sie Connect (Verbinden) aus, um eine Verbindung mit Ihrer Windows Server-Instance herzustellen.
6. Geben Sie an der Windows-Sicherheitsabfrage das Passwort für Ihre Windows-Server-Instance in das Textfeld Kennwort ein und wählen Sie dann OK aus.



7. Wählen Sie an der Eingabeaufforderung für die Remotedesktopverbindung Ja aus, um eine Verbindung herzustellen.



Sie sollten eine Seite ähnlich der folgenden sehen, wenn Sie sich erfolgreich mit Ihrer Instance verbunden haben:



Nächste Schritte

Wir empfehlen, das Administratorpasswort für Ihre Windows-Server-Instance in Amazon EC2 zu ändern. Dies entfernt die Zuordnung zwischen dem Standard-Lightsail-Schlüsselpaar und Ihrer Windows-Server-Instance in Amazon EC2. Weitere Informationen finden Sie unter Sichern einer Windows-Server-Instance in Amazon EC2, die aus einem Lightsail-Snapshot erstellt wurde.

Erstellen eines Snapshots Ihrer Lightsail-Windows Server-Instance

Ein Snapshot ist eine Kopie des Systemlaufwerks und der ursprünglichen Konfiguration einer Instance. Der Snapshot enthält Informationen wie Speicher, CPU, Festplattengröße und Datenübertragungsrate. Weitere Informationen finden Sie unter Snapshots.

Um einen Snapshot Ihrer Windows Server-Instance in Lightsail zu erstellen, erzeugen Sie zunächst einen Backup-Snapshot. Erstellen Sie anschließend einen zweiten Snapshot mit einem speziellen Dienstprogramm, das als System Preparation (Sysprep) bekannt ist. Sysprep generalisiert die Windows Server-Installation, so dass die Instance als Snapshot gesichert werden kann. Wenn Sie dann eine Instance aus diesem Snapshot erstellen, haben Sie eine Out-of-Box-Erfahrung, als ob Sie diese Windows-Instance zum ersten Mal ausführen würden.

Um einen Snapshot einer Linux- oder Unix-Instance zu erstellen, beachten Sie Erstellen eines Snapshots Ihrer Linux- oder Unix-Instance.

Inhalt

Schritt 1: Erstellen eines Backup-Snapshots vor Ausführung von Sysprep

Wenn Sie Sysprep ausführen, um einen Snapshot zu erstellen, werden systemspezifische Informationen aus Ihrer Instance entfernt. Dies kann unbeabsichtigte Folgen für die Anwendungen haben, die auf der Instance ausgeführt werden. Aus diesem Grund sollten Sie zuerst einen Backup-Snapshot vor dem Ausführen von Sysprep erstellen, um sicherzustellen, dass Sie einen alternativen Snapshot haben, wenn Fehler auftreten.

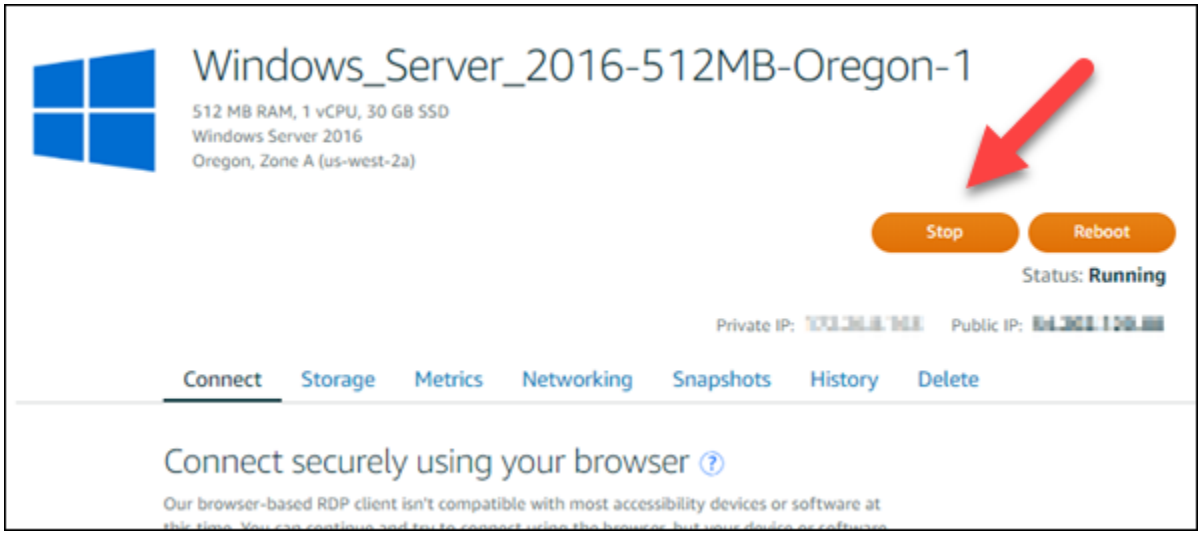
Wenn Sie einen Snapshot erstellen, bevor Sie Sysprep ausführen, haben Instances, die Sie mit dem Backup-Snapshot erstellen, das gleiche Administratorpasswort wie die Original-Instance.

Sie können sich nicht mit dem browserbasierten RDP-Client in der Lightsail-Konsole mit diesen Instances verbinden. Sie können sich jedoch mit Ihrem eigenen RDP-Client und demselben Administratorpasswort wie für die Original-Instance verbinden. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Ihrer Windows-Instance in Amazon Lightsail mithilfe des Remote-Desktop-Verbindungs-Clients auf einem Windows-Computer.

> **Important**
>
> Speichern Sie das Administratorpasswort der ursprünglichen Windows-Instance und an einem sicheren Ort. Sie benötigen dieses Administratorpasswort später, wenn etwas schief geht, und Sie erstellen eine Instance aus dem Snapshot, den Sie vor dem Ausführen von Sysprep erstellt haben.

So erstellen Sie einen Backup-Snapshot, bevor Sie Sysprep ausführen

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Startseite von Lightsail den Namen der Windows Server-Instance, für die Sie einen Snapshot erstellen möchten.
3. Wählen Sie Stop (Stopp) oben auf der Instance-Verwaltungsseite, um Ihre Instance zu stoppen.



> **Note**
>
> Wenn Sie eine Instance anhalten, ist jede Website oder jeder Service darauf solange nicht verfügbar, bis sie wieder gestartet wird.

4. Wählen Sie die Registerkarte Snapshots aus.
5. Wählen Sie im Abschnitt Manual snapshots (Manuelle Snapshots) der Seite Create snapshot (Snapshot erstellen) und geben Sie dann einen Namen für Ihren Snapshot ein.

   Ressourcennamen:

   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.
6. Wählen Sie Erstellen aus.
7. Wählen Sie in der Eingabeaufforderung erneut Create snapshot (Snapshot erstellen), um es zu bestätigen.

   Der Snapshot-Prozess dauert einige Minuten.
8. Nachdem der Snapshot erstellt wurde, wählen Sie Start oben auf der Instance-Verwaltungsseite, um Ihre Instance erneut zu starten.

Schritt 2: Verbindung mit Ihrer Instance und deren Beendigung mit Sysprep

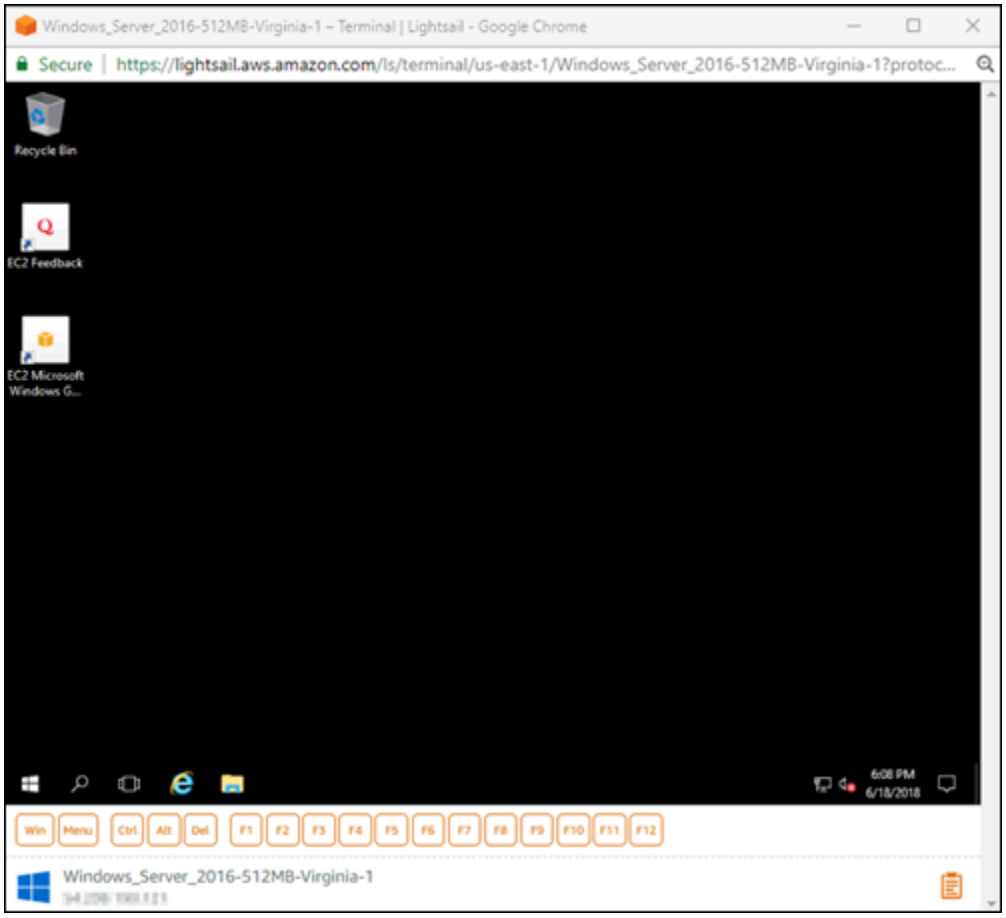
Jetzt, da Sie einen Backup-Snapshot erstellt haben, können Sie Sysprep auf Ihrer Windows Server-Instance auszuführen. Dadurch wird die Instance heruntergefahren, so dass Sie einen Snapshot erstellen können. Weitere Informationen über Sysprep finden Sie unter Sysprep-Übersicht in der Microsoft-Dokumentation.

In diesem Schritt stellen Sie eine Verbindung zu Ihrer Instance her und führen Sysprep über eine vorinstallierte Anwendung aus. Die Anwendung heißt EC2LaunchSettings unter Windows-Server-2019- und Windows-Server-2016-Instances und Ec2ConfigService-Einstellungen unter Windows-Server-2012-Instances.

So verbinden Sie sich mit Ihrer Instance und führen Sysprep aus

1. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using RDP (Verbinden mit RDP).

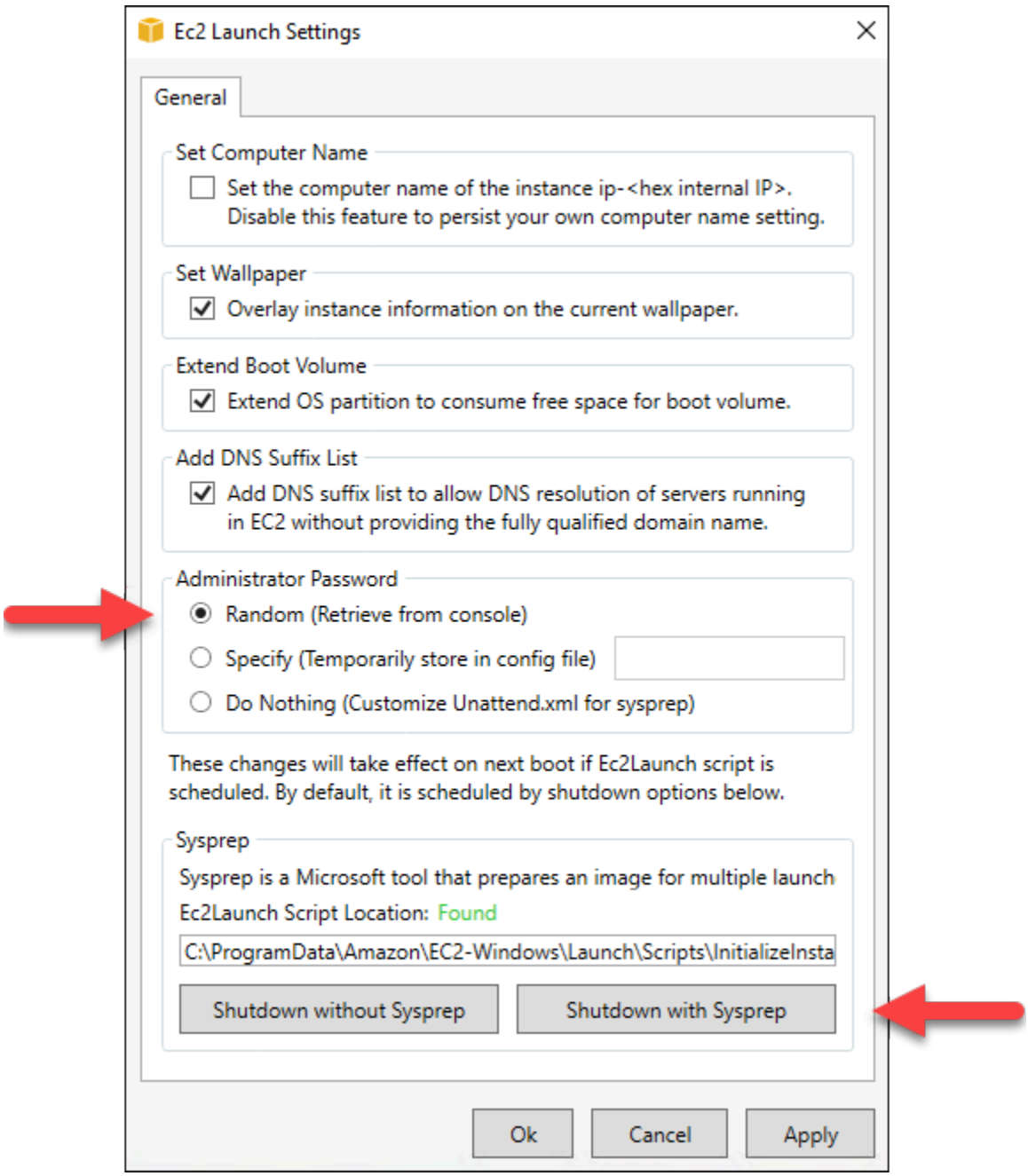
   Das browserbasierte RDP-Fenster wird geöffnet, wie im folgenden Beispiel gezeigt:



2. Wählen Sie in der Taskleiste das Windows-Symbol oder Win, um das Startmenü anzuzeigen.
3. Wählen Sie eine dieser Optionen aus:

   - Wählen Sie auf den Windows-Server-2019- und Windows-Server-2016-Instances Start und dann Ec2LaunchSettings.
   - Wählen Sie auf den Windows Server 2012-Instances Start und dann Ec2ConfigService Settings (Ec2ConfigService-Einstellungen).
4. Wählen Sie im Abschnitt Administrator-Passwort Random (Retrieve from console) (Beliebig (Abrufen von Konsole)) und anschließend Shutdown with Sysprep (Mit Sysprep herunterfahren).

   Bei den Ec2ConfigService-Einstellungen, die in Windows Server 2012-Instances vorhanden ist, sind die Optionen Random (Retrieve from console) (Beliebig (Abrufen von Konsole)) und Shutdown with Sysprep (Mit Sysprep herunterfahren) unter der Registerkarte Launch (Starten) aufgelistet.



5. Wählen Sie Yes (Ja), um zu bestätigen, dass Sie Sysprep ausführen und die Instance herunterfahren möchten.

   Ihre Instance beginnt mit der Ausführung von Sysprep, Ihre RDP-Verbindung wird heruntergefahren, und Ihre Lightsail-Instance stoppt nach einigen Minuten.

Schritt 3: Erstellen eines Snapshots nach Ausführung von Sysprep

Nachdem sich Ihre Instance in einem gestoppten Zustand befindet, erstellen Sie einen Snapshot in der Lightsail-Konsole. Wenn Sie nach dem Ausführen von Sysprep einen Snapshot Ihrer Windows Server-Instance erstellen, verfügen alle Instances, die Sie basierend auf dem Snapshot erstellen, über ein eindeutiges Administratorpasswort. Sie können sich mit diesen Instances verbinden, indem Sie den browserbasierten RDP-Client in der Lightsail-Konsole verwenden.

So erstellen Sie einen Snapshot in der Lightsail-Konsole

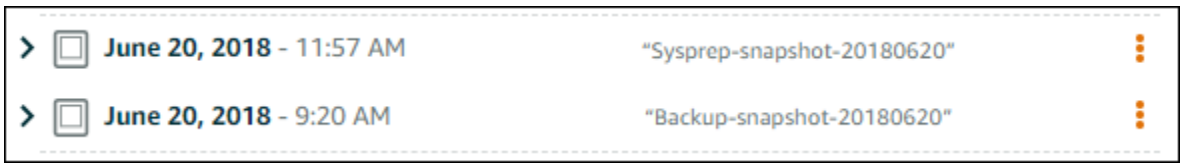
1. Wechseln Sie zurück zur Lightsail-Konsole.
2. Wählen Sie auf der Instance-Verwaltungsseite für Ihre Windows Server-Instance die Registerkarte Snapshots aus.
3. Wählen Sie im Abschnitt Manual snapshots (Manuelle Snapshots) der Seite Create snapshot (Snapshot erstellen) und geben Sie dann einen Namen für Ihren Snapshot ein.

   Ressourcennamen:

   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.
4. Wählen Sie Erstellen aus.
5. Wählen Sie in der Eingabeaufforderung Create snapshot (Snapshot erstellen) aus, um zu bestätigen, dass Sie die Instance für den Snapshot vorbereitet haben.

   Der Snapshot-Prozess dauert einige Minuten.
6. Nachdem der Snapshot erstellt wurde, wählen Sie Start oben auf der Instance-Verwaltungsseite, um Ihre Instance erneut zu starten.

   Zu diesem Zeitpunkt sollten Sie zwei Snapshots Ihrer Windows Server-Instance haben, wie im folgenden Beispiel gezeigt:



Verwenden Sie den Sysprep-Snapshot, um neue Instances zu erstellen. Verwenden Sie den Backup-Snapshot nur dann, wenn die ursprüngliche Instance nach dem Ausführen von Sysprep nicht wie erwartet funktioniert.

Nächste Schritte

Nun, da Sie die Sysprep- und Backup-Snapshots haben, folgen Sie den nächsten Schritten, die Sie ausführen sollten:

- Verbinden Sie sich mit Ihrer ursprünglichen Instance und überprüfen Sie, ob Ihre Anwendungen nach der Ausführung von Sysprep wie erwartet funktionieren. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-Server-Instance in Amazon Lightsail.
- Erstellen Sie mit dem Sysprep-Snapshot eine neue Instance, verbinden Sie sich mit ihr und überprüfen Sie, ob Ihre Anwendungen auf der neuen Instance wie erwartet funktionieren. Weitere Informationen finden Sie unter Erstellen einer Instance aus einem Snapshot.
- Löschen Sie Ihren Backup-Snapshot, nachdem Sie verifiziert haben, dass die Original-Instance nach dem Ausführen von Sysprep wie erwartet funktioniert. Weitere Informationen finden Sie unter Löschen von Snapshots.
- Wenn Ihre Instance nach dem Ausführen von Sysprep nicht wie erwartet funktioniert, befolgen Sie die Schritte in Erstellen einer Instance aus einem Snapshot, um eine neue Instance aus dem Backup-Snapshot zu erstellen.

Sichern Sie eine Windows-Server-Instance in Amazon EC2, die aus einem Lightsail-Snapshot erstellt wurde

Um die Sicherheit einer Windows-Server-Instance in Amazon Elastic Compute Cloud (Amazon EC2) zu verbessern, die aus einem Amazon Lightsail-Snapshot erstellt wurde, empfehlen wir Ihnen, das Standard-Administratorpasswort zu ändern. Dadurch wird die Zuordnung zwischen Ihren Lightsail-Schlüsselpaaren und Ihrer neuen Windows-Server-Instance in Amazon EC2 aufgehoben.

> **Note**
>
> Wenn Sie Linux- oder Unix-Instances in Amazon EC2 aus einem Lightsail-Snapshot erstellt haben, dann sollten Sie einige Schritte ausführen, um diese Instances zu sichern. Weitere

Informationen finden Sie unter Sichern einer Amazon-EC2-Linux- oder Unix-Instance, die aus einem Lightsail-Snapshot erstellt wurde.

Inhalt

Herstellen einer Verbindung zu Ihrer Windows-Server-Instance in Amazon EC2

Um Ihr Windows Server-Administratorpasswort zu ändern, verbinden Sie sich mit Ihrer Windows-Server-Instance in Amazon EC2 über das Remote Desktop Protocol (RDP). Weitere Informationen, wie Sie sich mit Ihrer Instance verbinden, finden Sie unter Verbindung zu einer Windows-Server-Instance in Amazon EC2, die aus einem Lightsail-Snapshot erstellt wurde.

Fahren Sie mit dem Abschnitt Ändern des Standard-Administratorpassworts Ihrer Windows-Server-Instance in Amazon EC2 in diesem Handbuch fort, wenn Sie die Verbindung zu Ihrer Instance in Amazon EC2 hergestellt haben.

Ändern des Standard-Administratorpassworts Ihrer Windows-Server-Instance in Amazon EC2

Ändern Sie das Standardpasswort auf Ihrer Windows-Server-Instance, um die Zuordnung zwischen Ihren Lightsail-Schlüsselpaaren und Ihrer neuen Windows-Server-Instance in Amazon EC2 aufzuheben.

Wie Sie das Standard-Administratorpassworts Ihrer Windows-Server-Instance in Amazon EC2 ändern

1. Nachdem Sie eine RDP-Verbindung zu Ihrer Instance hergestellt haben, öffnen Sie eine Eingabeaufforderung und geben Sie den folgenden Befehl ein.

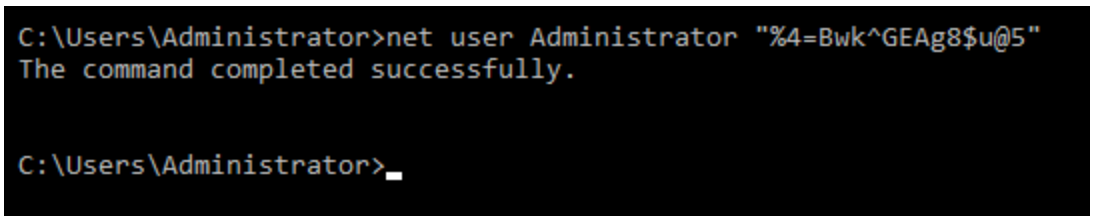
   ```
   net user Administrator "Password"
   ```

   Ersetzen Sie im Befehl *Password* durch Ihr neues Passwort.

   Beispiel:

```
net user Administrator "%4=Bwk^GEAg8$u@5"
```

Das Ergebnis sollte in etwa wie folgt aussehen:



2. Speichern Sie das neue Passwort an einem sicheren Ort. Sie können das neue Passwort nicht über die Amazon-EC2-Konsole abrufen. Sie können nur das Standard-Passwort über die Konsole abrufen. Wenn Sie versuchen, sich mit dem Standard-Passwort mit der Instance zu verbinden, nachdem Sie es geändert haben, erscheint eine Fehlermeldung, dass Ihre Anmeldeinformationen nicht funktioniert haben.

   Wenn Sie Ihr Passwort verlieren oder es abläuft, können Sie ein neues Passwort generieren. Informationen zum Zurücksetzen des Passworts finden Sie unter Zurücksetzen eines Windows-Administratorpassworts, das verloren oder abgelaufen ist in der Amazon-EC2-Dokumentation.

Erfahren Sie, wie Sie eine Linux- oder Unix-Instance in Amazon EC2 sichern können, die aus einem Lightsail-Snapshot erstellt wurde

Amazon Lightsail und Amazon Elastic Compute Cloud (Amazon EC2) verwenden Kryptografie für öffentliche Schlüssel, um Anmeldeinformationen zu ver- und entschlüsseln. Bei der Kryptografie für öffentliche Schlüssel werden öffentliche Schlüssel eingesetzt, um Daten wie ein Passwort zu verschlüsseln. Der Empfänger entschlüsselt diese Daten dann mit einem privaten Schlüssel. Der öffentliche und der private Schlüssel werden als Schlüsselpaar bezeichnet.

Wenn Sie eine Linux- oder Unix-Lightsail-Instance nach EC2 exportieren, enthält die neue EC2-Instance Restschlüssel aus dem Lightsail-Service. Als bewährte Methode für die Sicherheit sollten Sie nicht benutzte Schlüssel aus Ihrer Instance entfernen.

Um die Sicherheit einer Linux- oder Unix-Instance in EC2 zu verbessern, die aus einem Lightsail-Snapshot erstellt wurde, empfehlen wir Ihnen, nach dem Erstellen der Instance die folgenden Aktionen durchzuführen:

- Entfernen und ersetzen Sie den Lightsail-Standardschlüssel, wenn Sie ihn zur Verbindung mit der Quell-Instance in Lightsail verwendet haben. Der Lightsail-Standardschlüssel ist in Ihrer Amazon-EC2-Instance nicht vorhanden, wenn Sie Ihren eigenen Schlüssel verwendet haben, um sich mit Ihrer Instance zu verbinden, oder einen Schlüssel für Ihre Instance in der Lightsail-Konsole erstellt haben.
- Entfernen Sie den Lightsail-Systemschlüssel, auch bekannt als der `lightsail_instance_ca.pub`-Schlüssel. Dieser Schlüssel auf Linux- und Unix-Instances ermöglicht es dem Lightsail-browserbasierten SSH-Client, sich zu verbinden. Der `lightsail_instance_ca.pub`-Schlüssel wird automatisch entfernt, wenn eine EC2-Instance mithilfe der Seite Eine Amazon-EC2-Instance erstellen in der Lightsail-Konsole oder der Lightsail-API erstellt wird.

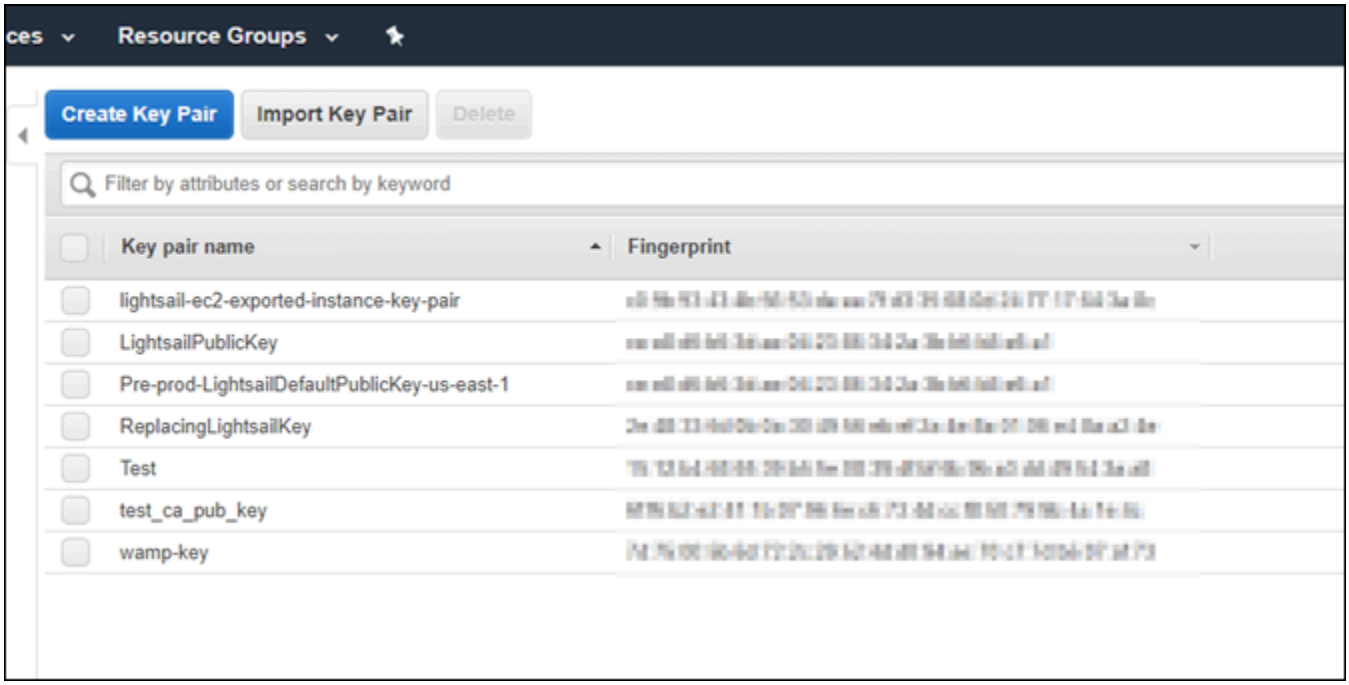
Inhalt

Erstellen eines privaten Schlüssels mit Amazon EC2

Erstellen Sie mit der Amazon-EC2-Konsole ein neues Schlüsselpaar, um das Lightsail-Standard-Schlüsselpaar zu ersetzen.

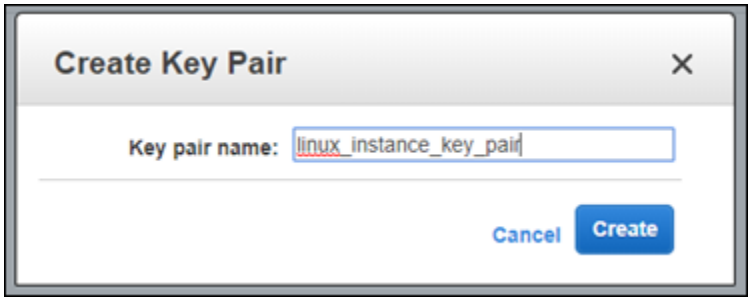
Wie Sie einen privaten Schlüssel mit Amazon EC2 erstellen

1. Melden Sie sich bei der Amazon-EC2-Konsole an.
2. Wählen Sie im linken Navigationsbereich Key Pairs (Schlüsselpaare).
3. Wählen Sie Create Key Pair (Schlüsselpaar erstellen) aus.



4. Geben Sie einen Namen für den Schlüssel in das Textfeld Key pair name (Schlüsselpaarname) ein und wählen Sie dann Create (Erstellen).

   Der neue private Schlüssel wird automatisch heruntergeladen. Notieren Sie sich, wo der private Schlüssel gespeichert wird. Sie benötigen ihn im folgenden Abschnitt Erstellen des öffentlichen Schlüssels mit PuTTYgen in diesem Handbuch, um einen öffentlichen Schlüssel zu erstellen.



Erstellen des öffentlichen Schlüssels mit PuTTYgen

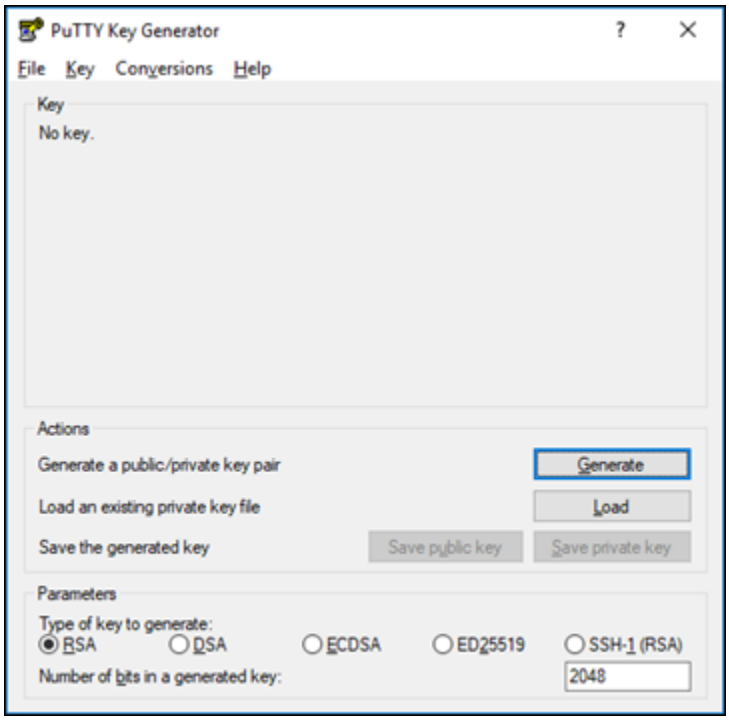
PuTTYgen ist ein Werkzeug, das in PuTTY enthalten ist. Verwenden Sie PuTTYgen, um den Text des öffentlichen Schlüssels zu generieren, den Sie später in diesem Handbuch zu Ihrer Instance hinzufügen.

> **Note**
>
> Weitere Informationen zur Konfiguration von PuTTY für die Verbindung mit Ihrer Linux- oder Unix-Instance finden Sie unter Verbinden mit einer Amazon EC2 Linux- oder Unix-Instance in , die aus einem Lightsail-Snapshot erstellt wurde.

So erstellen Sie den öffentlichen Schlüssel mit PuTTYgen

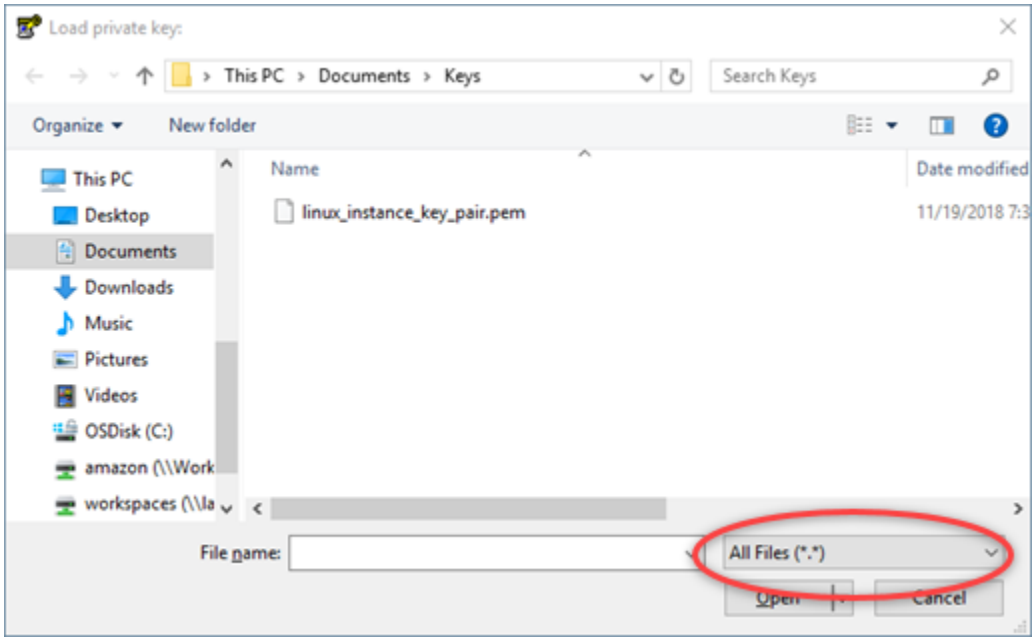
1. Starten Sie PuTTYgen.

   Wählen Sie beispielsweise das Windows-Startmenü aus. Wählen Sie dann Alle Programme, PuTTY und PuTTYgen aus.



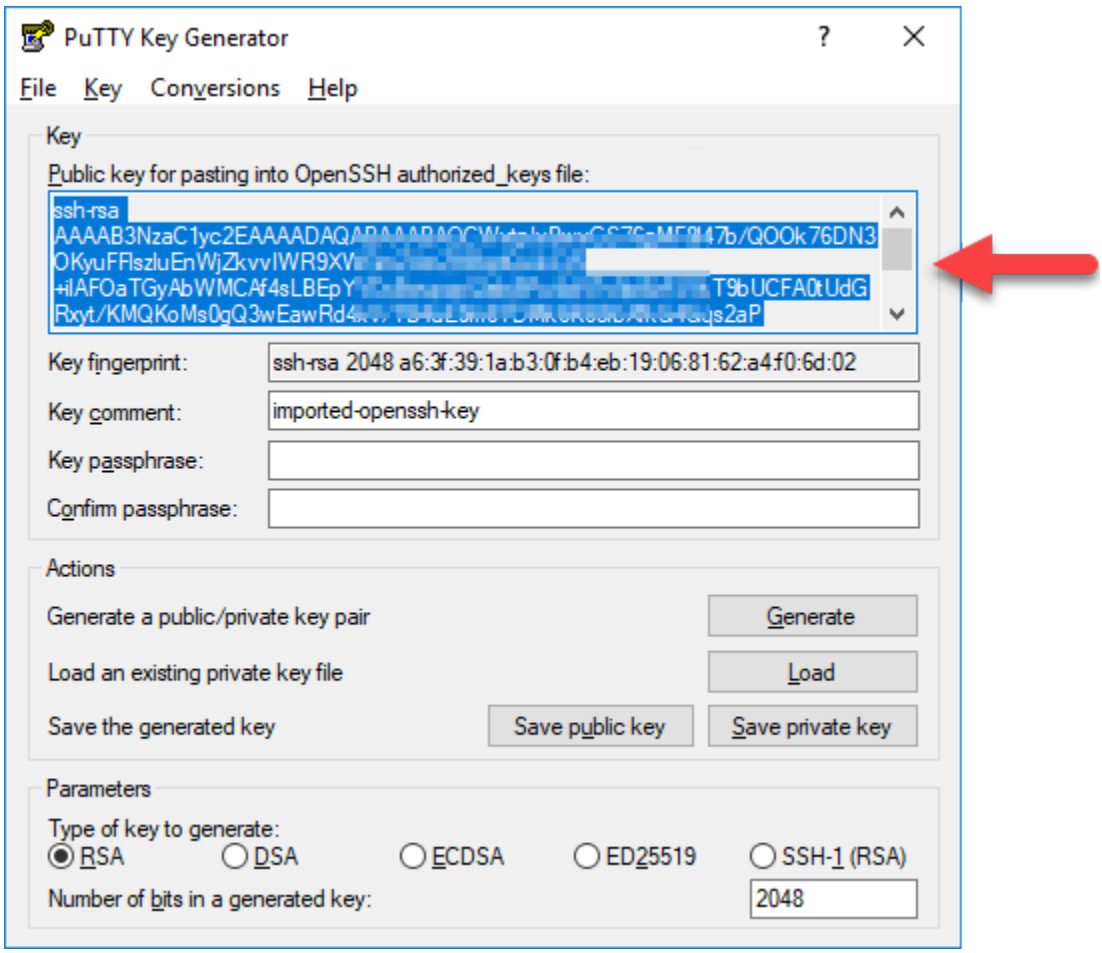
2. Wählen Sie Load (Laden) aus.

   PuTTYgen zeigt standardmäßig nur Dateien mit der Erweiterung PPK an. Damit Sie die PEM-Datei finden, wählen Sie die Option zur Anzeige aller Dateitypen.



3. Navigieren Sie zum Speicherort Ihres privaten Schlüssels, der weiter oben in diesem Handbuch erstellt wurde. Wählen Sie den privaten Schlüssel und dann Open (Öffnen).
4. Nachdem PuTTYgen bestätigt hat, dass Sie den Schlüssel erfolgreich importiert haben, wählen Sie OK aus.
5. Markieren Sie den Inhalt des Textfeldes Public key (Öffentlicher Schlüssel) und kopieren Sie ihn in die Zwischenablage, indem Sie Ctrl+C (Strg+C) drücken, wenn Sie Windows verwenden, oder Cmd+C, wenn Sie MacOS verwenden.

   Öffnen Sie einen Texteditor, wie beispielsweise Notepad oder TextEdit, und fügen Sie den Text des öffentlichen Schlüssels ein, indem Sie Ctrl+V (Strg+V) drücken, wenn Sie Windows verwenden, oder Cmd+V, wenn Sie MacOS verwenden. Speichern Sie die Datei mit Ihrem öffentlichen Schlüsseltext. Sie werden ihn später noch in diesem Handbuch benötigen.



6. Fahren Sie mit dem Abschnitt Verbinden mit Ihrer Linux- oder Unix-Instance in Amazon EC2 dieses Handbuchs fort, um eine Verbindung zu Ihrer EC2-Instance herzustellen und den öffentlichen Schlüssel hinzuzufügen.

Verbinden mit Ihrer Linux- oder Unix-Instance in Amazon EC2

Verbinden Sie sich mit Ihrer Linux- oder Unix-Instance in Amazon EC2 mit SSH, um den Lightsail-Standardschlüssel und den Systemschlüssel zu entfernen. Weitere Informationen finden Sie unter Verbinden mit einer Linux- oder Unix-Instance in Amazon EC2, die aus einem Amazon Lightsail-Snapshot erstellt wurde.

Fahren Sie mit dem Abschnitt Hinzufügen des öffentlichen Schlüssels zu Ihrer Instance und Testen der Verbindung in diesem Handbuch fort, wenn Sie mit Ihrer Instance in Amazon EC2 verbunden sind.

Hinzufügen des öffentlichen Schlüssels zu Ihrer Instance und Testen der Verbindung

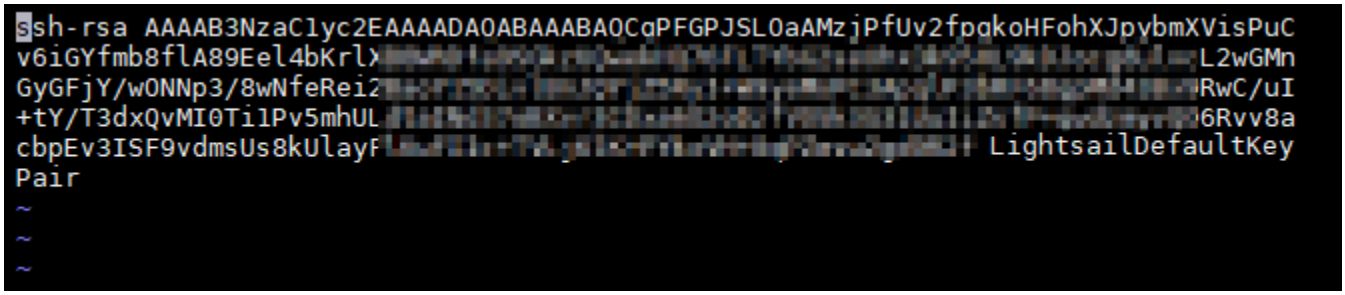
Der Inhalt des öffentlichen Schlüssels wird in der Datei `~/.ssh/authorized_keys` auf Linux- und Unix-Instances gespeichert. Bearbeiten Sie die Datei und entfernen und ersetzen Sie den Lightsail-Standardschlüssel aus Ihrer Linux- oder Unix-Instance in Amazon EC2.

So fügen Sie den öffentlichen Schlüssel zu Ihrer Instance hinzu und testen die Verbindung

1. Nachdem Sie eine SSH-Verbindung zu Ihrer Instance hergestellt haben, geben Sie den folgenden Befehl ein, um die Datei `authorized_keys` mit dem Vim-Texteditor zu bearbeiten.

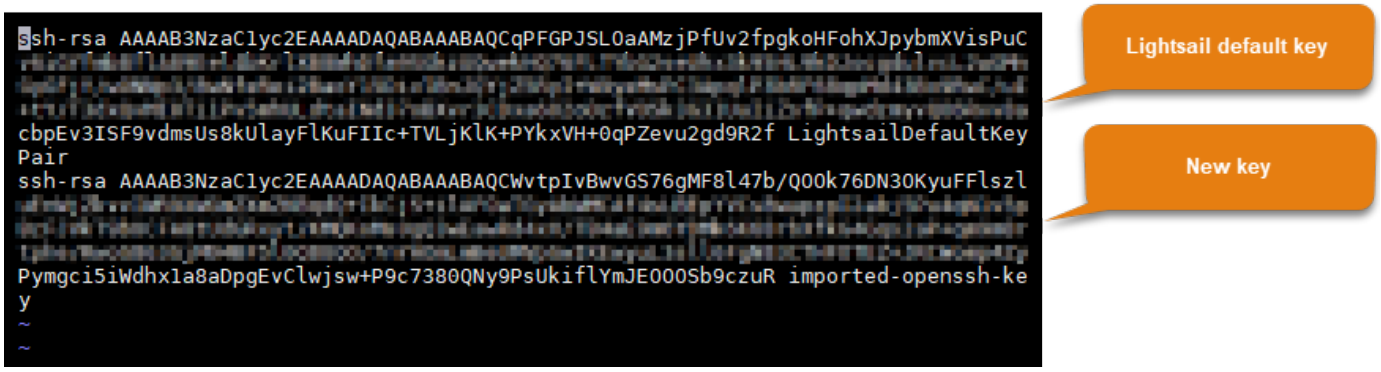
   ```
   sudo vim ~/.ssh/authorized_keys
   ```

   > **Note**
   >
   > Diese Schritte verwenden Vim zu Demonstrationszwecken. Sie können für diese Schritte jedoch jeden beliebigen Texteditor verwenden.

2. Drücken Sie die Taste `I`, um in den Einfügemodus im Vim-Editor zu gelangen.
3. Fügen Sie eine zusätzliche Zeile nach dem Lightsail-Standardschlüssel ein.
4. Kopieren und fügen Sie den Text des öffentlichen Schlüssels ein, den Sie zuvor diesem Handbuch folgend gespeichert haben.

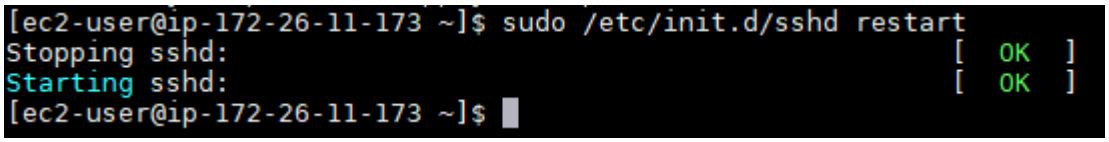
   Das Ergebnis sollte wie folgt aussehen:



5. Drücken Sie die Taste ESC, und geben Sie dann `:wq!` ein, um Ihre Änderungen zu schreiben oder zu speichern und Vim zu beenden.
6. Geben Sie den folgenden Befehl ein, um den Open SSH-Server neu zu starten:

```
sudo /etc/init.d/sshd restart
```

Das Ergebnis sollte in etwa wie folgt aussehen:



Ihr neuer öffentlicher Schlüssel ist nun zu Ihrer Instance hinzugefügt. Um das neue Schlüsselpaar zu testen, trennen Sie die Verbindung zu Ihrer Instance. Konfigurieren Sie PuTTY so, dass es Ihren neuen privaten Schlüssel anstelle des Lightsail-Standardschlüssels verwendet. Wenn Sie sich mit Ihrem neuen Schlüsselpaar erfolgreich mit Ihrer Instance verbinden können, fahren Sie mit dem Abschnitt Entfernen des Lightsail-Standardschlüssels in diesem Handbuch fort, um den Lightsail-Standardschlüssel zu entfernen.

Entfernen des Lightsail-Standardschlüssels

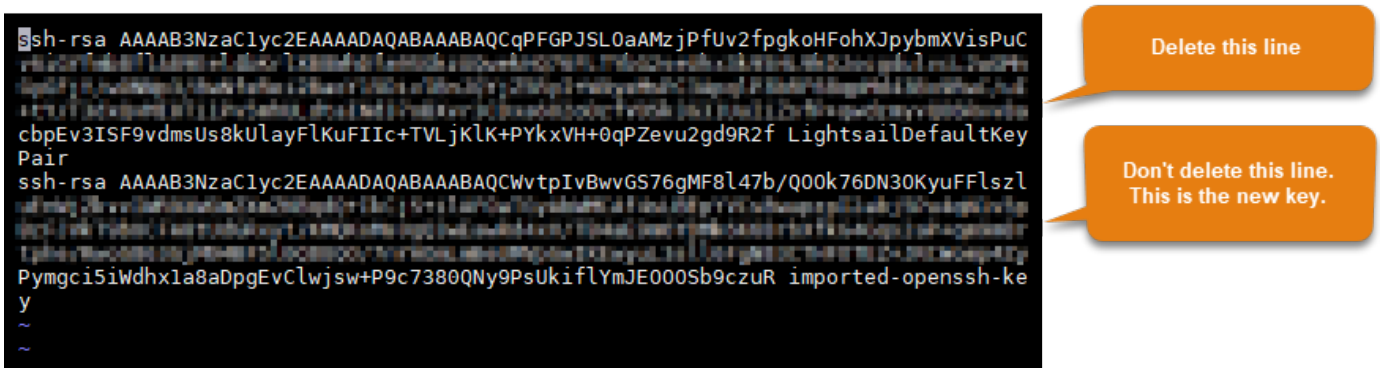
Entfernen Sie den Lightsail Standardschlüssel, nachdem Sie Ihrer Instance einen neuen öffentlichen Schlüssel hinzugefügt und sich mit dem neuen Schlüsselpaar erfolgreich mit der Instance verbunden haben.

So entfernen Sie den Lightsail-Standardschlüssel

1. Nachdem Sie eine SSH-Verbindung zu Ihrer Instance hergestellt haben, geben Sie den folgenden Befehl ein, um `authorized_keys file` mit dem Vim-Texteditor zu bearbeiten.

```
sudo vim ~/.ssh/authorized_keys
```

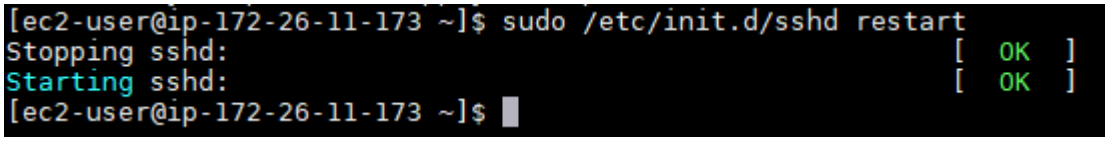
2. Drücken Sie die Taste `I`, um in den Einfügemodus im Vim-Editor zu gelangen.
3. Löschen Sie die Zeile, die mit `LightsailDefaultKeyPair` endet. Das ist der Lightsail-Standardschlüssel.



4. Drücken Sie die Taste `ESC`, und geben Sie dann `:wq!` ein, um Ihre Änderungen zu schreiben oder zu speichern und Vim zu beenden.
5. Geben Sie den folgenden Befehl ein, um den Open SSH-Server neu zu starten:

```
sudo /etc/init.d/sshd restart
```

Das Ergebnis sollte in etwa wie folgt aussehen:



Der Lightsail-Standardschlüssel ist nun von Ihrer Instance entfernt. Ihre Instance wird jetzt Verbindungen verweigern, die den Lightsail-Standardschlüssel verwenden. Fahren Sie mit dem Abschnitt Entfernen des Lightsail-Systemschlüssels in diesem Handbuch fort, um den Lightsail-Systemschlüssel zu entfernen.

Entfernen des Lightsail-Systemschlüssels

Der Lightsail-Systemschlüssel, bekannt auch als `lightsail_instance_ca.pub`-Schlüssel, auf Linux- und Unix-Instances ermöglicht es dem Lightsail-browserbasierten SSH-Client, sich zu verbinden. Führen Sie die folgenden Schritte aus, um den `lightsail_instance_ca.pub`-Schlüssel aus Ihrer Linux- oder Unix-Instance in Amazon EC2 zu entfernen, und bearbeiten Sie die

Datei `/etc/ssh/sshd_config`. Die `/etc/ssh/sshd_config`-Datei definiert die Parameter für SSH-Verbindungen zu Ihrer Instance.

So entfernen Sie den Lightsail-Systemschlüssel

1. Geben Sie in einem mit Ihrer Instance verbundenen SSH-Terminalfenster den folgenden Befehl ein, um den Schlüssel `lightsail_instance_ca.pub` zu entfernen:

   ```
   sudo rm -r /etc/ssh/lightsail_instance_ca.pub
   ```

2. Geben Sie den folgenden Befehl ein, um die Datei `sshd_config` mit dem Vim-Texteditor zu bearbeiten.

   ```
   sudo vim /etc/ssh/sshd_config
   ```

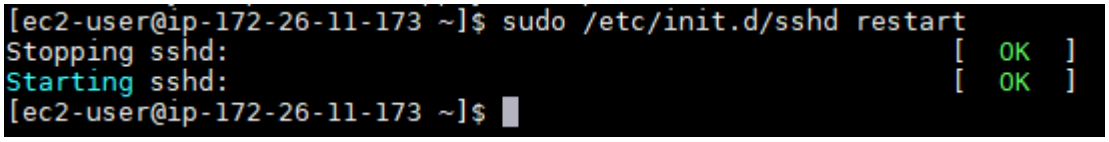
3. Drücken Sie die Taste `I`, um in den Einfügemodus im Vim-Editor zu gelangen.
4. Löschen Sie den folgenden Text aus der Datei, sofern vorhanden:

   ```
   TrustedUserCAKeys /etc/ssh/lightsail_instance_ca.pub
   ```

5. Drücken Sie die Taste `ESC`, und geben Sie dann `:wq!` ein, um Ihre Änderungen zu schreiben oder zu speichern und Vim zu beenden.
6. Geben Sie den folgenden Befehl ein, um den Open SSH-Server neu zu starten:

   ```
   sudo /etc/init.d/sshd restart
   ```

   Das Ergebnis sollte in etwa wie folgt aussehen:

   Der `lightsail_instance_ca.pub`-Schlüssel ist nun von Ihrer Instance entfernt. Die zugehörige Datei `sshd_config` wird aktualisiert, um diesen Schlüssel auszuschließen.

Verwaltung Ihrer Lightsail-Instance

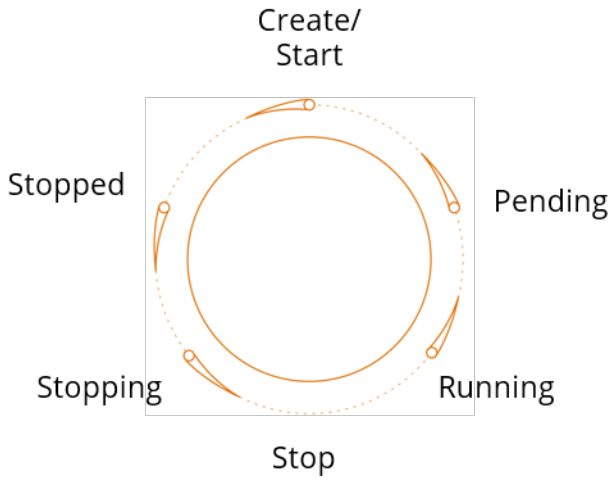
In Lightsail, wird Ihr VPS (Virtual Private Server) als Instance bezeichnet. Sie können eine Verbindung mit Ihrer Instance herstellen, Ihre Ports und Firewall-Einstellungen verwalten, Metriken

anzeigen, Ihrer Instance eine statische IP-Adresse zuordnen und vieles andere mehr. Wählen Sie eine Aufgabe aus, um zu erfahren, wie Sie das meiste aus Ihrer Instance machen:

- Verbinden mit Ihrer Linux- oder Unix-Instance
- Metriken anzeigen
- Eine statische IP-Adresse erstellen und einer Instance zuordnen
- Firewall und Ports
- Erstellen eines Snapshots Ihrer Linux- oder Unix-Instance
- Starten, Stoppen oder Neustarten Ihrer Instance
- Stoppen Ihrer Instance erzwingen

Eine Lightsail-Instance starten, anhalten oder neustarten

Wenn Lightsail Ihre Instance erstellt, geht Ihre Maschine in den Status Pending (Ausstehend), bevor sie den Status Running (Ausführung) annimmt. Nachdem die Instance ausgeführt wird, können Sie sie neu starten oder anhalten und dann neu starten. Der Zyklus sieht wie folgt aus:



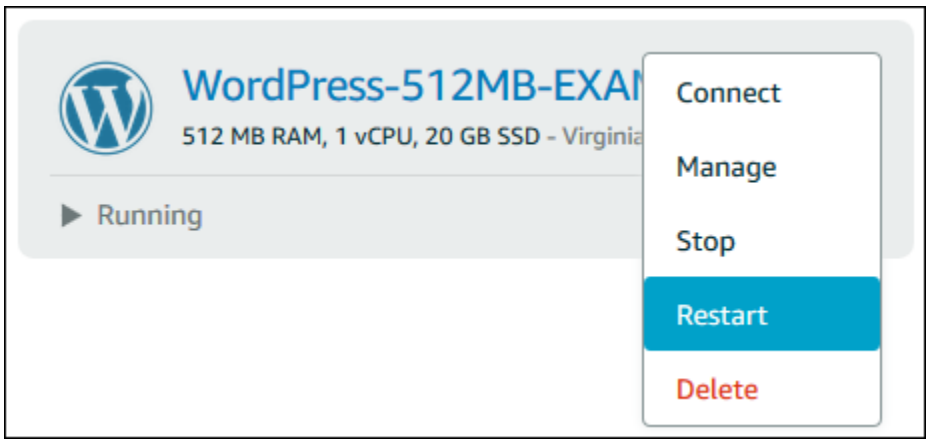
Sie sehen die Instance-Status, wenn Sie Ihre Instance verwalten oder Ihre Instance auf der Website anzeigen.

> **Important**
>
> Die standardmäßige öffentliche IPv4-Adresse, die Ihrer Instance beim Erstellen zugewiesen wird, ändert sich beim Anhalten und Starten Ihrer Instance. Sie können optional eine statische IPv4-Adresse erstellen und an Ihre Instance anfügen. Die statische IPv4-Adresse ersetzt

die standardmäßige öffentliche IPv4-Adresse Ihrer Instanz und bleibt unverändert, wenn Sie die Instance anhalten und starten. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

Starten Sie Ihre Instance neu, während dies ausgeführt wird

- Wählen Sie auf der Startseite die Instance, die Sie neu starten möchten, oder wählen Sie Restart (Neu starten) aus dem Menü der Instance-Verwaltung.

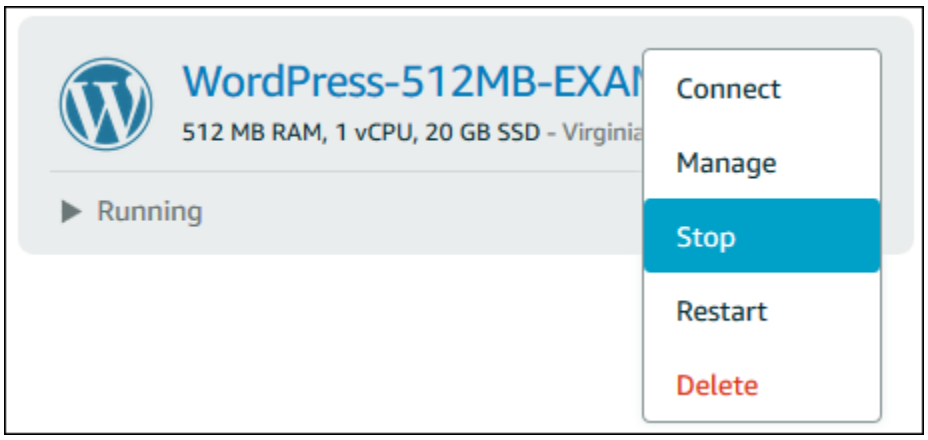


Wenn Sie Ihre Instance auf der Seite der Instance-Verwaltung anzeigen, wählen Sie Restart (Neu starten) und dann Confirm (Bestätigen), wenn Sie dazu aufgefordert werden.

> **Note**
>
> Um einen Restart (Neustart) Ihrer Instance durchzuführen, muss diese sich im Status Running (Ausführung) befinden.

Eine ausgeführte Instance anhalten

- Wählen Sie auf der Startseite die Instance, die Sie anhalten möchten, oder wählen Sie Stop (Anhalten) aus dem Menü der Instance-Verwaltung.

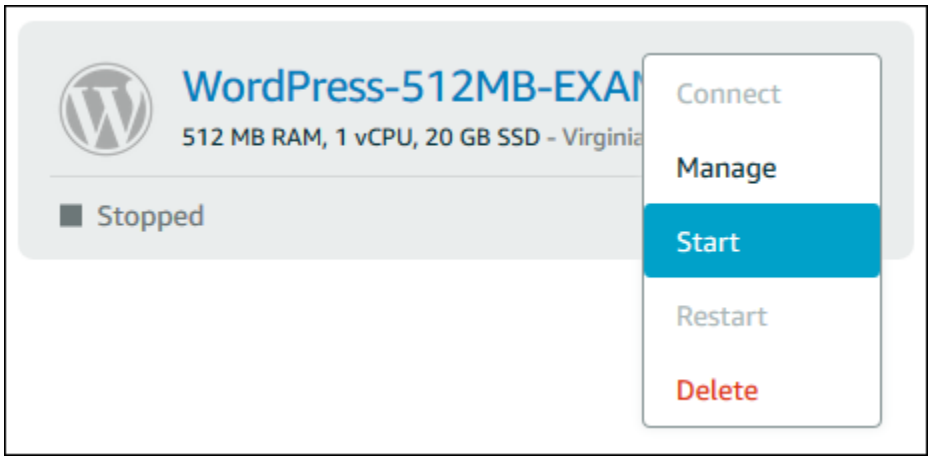


Wenn Sie Ihre Instance auf der Seite der Instance-Verwaltung anzeigen, wählen Sie Stop (Anhalten) und dann Confirm (Bestätigen), sobald Sie dazu aufgefordert werden.

> **Note**
>
> Um einen Stop (Anhalten) Ihrer Instance durchzuführen, muss sich diese im Status Running (Ausführung) befinden.

Starten Ihrer Instance, nachdem sie angehalten wurde

- Wählen Sie auf der Startseite die Instance, die Sie starten möchten, oder wählen Sie Start (Starten) aus dem Menü der Instance-Verwaltung.



Wenn Sie Ihre Instance auf der Seite der Instance-Verwaltung anzeigen, wählen Sie Start (Starten).

> **Note**
>
> Um einen Start Ihrer Instance durchzuführen, muss sich diese im Status Stopped (Angehalten) befinden.

Aktualisieren von Amazon-EC2-Instances für verbessertes Netzwerk

Einige Lightsail-Instances sind mit den EC2-Instance-Typ der aktuellen Generation (T3, M5, C5 oder R5) nicht kompatibel, da sie für das erweiterte Netzwerk nicht aktiviert sind. Wenn Ihre Quell-Lightsail-Instance inkompatibel ist, müssen Sie beim Erstellen einer EC2-Instance aus Ihrem exportierten Snapshot einen Instance-Typ der vorherigen Generation (T2, M4, C4 oder R4) auswählen. Diese Instance-Typ-Optionen werden Ihnen beim Erstellen einer EC2-Instance mithilfe der Seite Erstellen einer Amazon-EC2-Instance in der Lightsail-Konsole angezeigt.

> **Note**
>
> Weitere Informationen zu erweiterten Netzwerken finden Sie unter Erweiterte Netzwerke unter Linux oder Erweiterte Netzwerke unter Windows in der Amazon-EC2-Dokumentation.

Um die EC2-Instance-Typen der neuesten Generation zu verwenden, wenn die Quell-Instance Lightsail inkompatibel ist, müssen Sie die neue EC2-Instance mit einem Instance-Typ der vorherigen Generation (T2, M4, C4 oder R4) erstellen, den Netzwerktreiber auf Ihrer Instance aktualisieren und die Instance dann auf den gewünschten Instance-Typ der aktuellen Generation aktualisieren.

Voraussetzungen

Sie müssen eine Amazon-EC2-Instance aus einem exportiertenLightsail -Snapshot erstellen. Wenn Ihre Lightsail-Instance nicht kompatibel ist, wählen Sie einen Instance-Typ einer älteren Generation (T2-, M4-, C4- oder R4) beim Erstellen der Amazon-EC2-Instance aus. Weitere Informationen finden Sie unter Erstellen von Amazon-EC2-Instances aus exportierten Snapshots in Lightsail.

Nachdem Ihre neue EC2-Instance erstellt wurde und ausgeführt wird, fahren Sie mit dem Abschnitt Aktivieren des erweiterten Netzwerks über den Elastic Network Adapter in diesem Handbuch fort, um zu erfahren, wie Sie eine erweiterte Vernetzung aktivieren können.

Aktivieren des erweiterten Netzwerks über den Elastic Network Adapter

Nachdem Ihre neue Instance eingerichtet ist und ausgeführt wird, lesen Sie eine der folgenden Anleitungen in der Amazon-EC2-Dokumentation, um ein erweitertes Netzwerk mit dem Elastic Network Adapter (ENA) zu aktivieren:

- Aktivieren eines erweiterten Netzwerks mit dem ENA in Linux
- Aktivieren eines erweiterten Netzwerks mit dem ENA in Windows-Instances

Aktualisieren Sie Ihren Instance-Typ

Nachdem Sie das erweiterte Netzwerk aktiviert haben, können Sie den Instance-Typ aktualisieren, indem Sie den Anweisungen in einer der folgenden Anleitungen folgen:

- Für Windows Server-Instances – Migration auf Instance-Typen der neuesten Generation
- Für Linux- oder Unix-Instances – Ändern des Instance-Typs

Erweitern des Speicherplatzes Ihrer Lightsail-Windows-Server-Instance

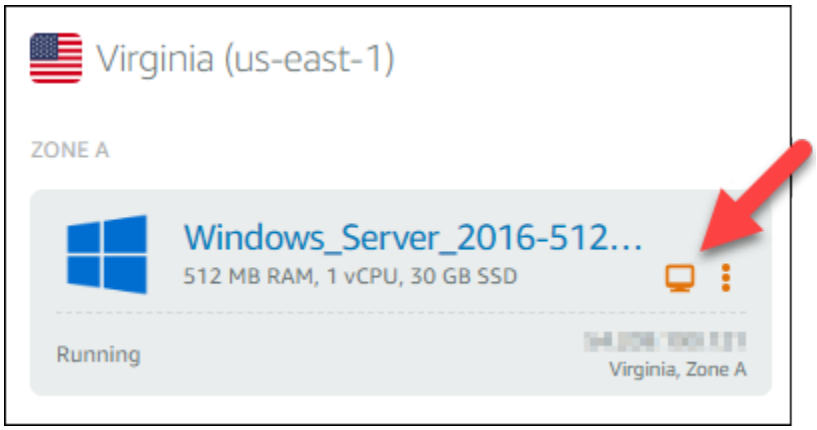
Wenn Sie einen Snapshot verwendet haben, um eine neue Windows Server-Instance mit einem größeren Plan zu erstellen, können Sie feststellen, dass der verfügbare Speicherplatz kleiner ist als der im Plan angegebene. Dies liegt typischerweise daran, dass der zusätzliche Speicherplatz, der durch den größeren Plan bereitgestellt wird, nicht zugewiesen wurde. Er wird daher vom aktiven Volume nicht genutzt. Die Schritte in diesem Thema zeigen Ihnen, wie Sie das Dateisystem Ihrer Windows Server-Instance erweitern können, um den maximal verfügbaren Speicherplatz zu nutzen.

> **Note**
>
> Dieses Szenario tritt nur auf, wenn Sie eine Windows Server-Instance auf Grundlage eines Snapshots erstellen, der vor der Ausführung des Dienstprogramms System Preparation (Sysprep) erstellt wurde. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Windows-Server-Instance.

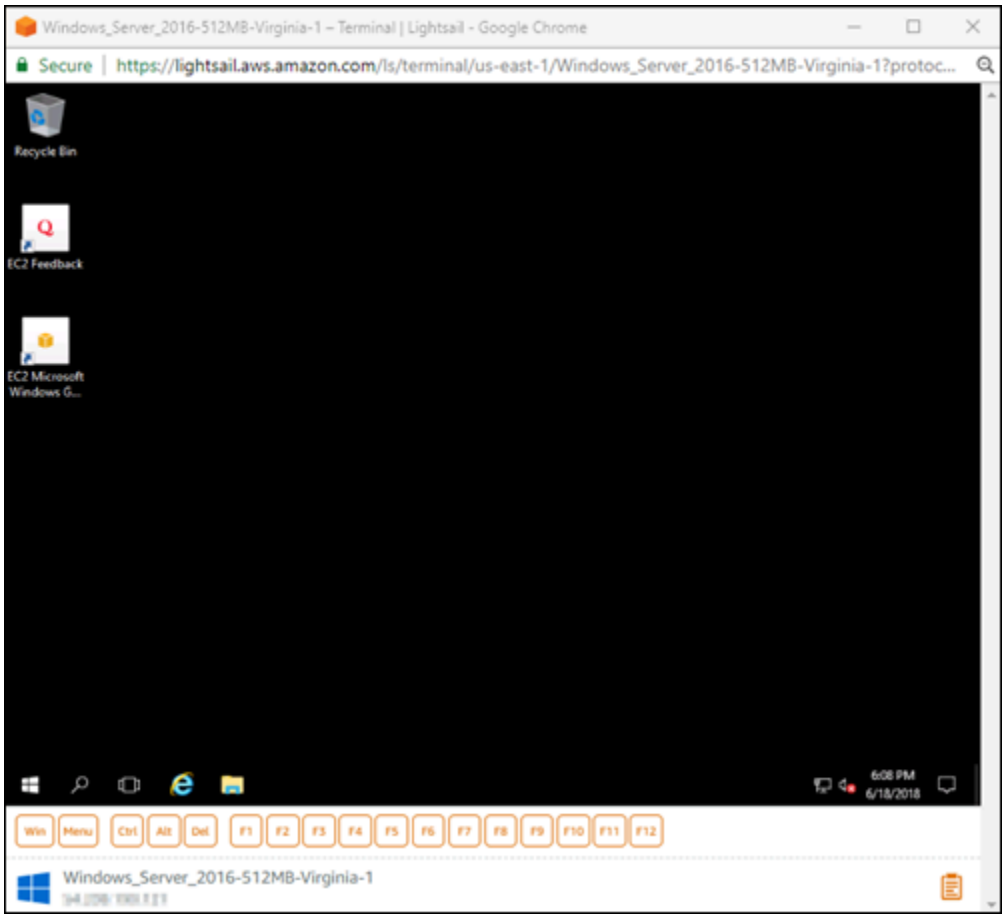
So erweitern Sie das Dateisystem für eine Windows Server-Instance

1. Melden Sie sich an der Lightsail-Konsole an.

2. Wählen Sie auf der Startseite von Lightsail das RDP-Client-Symbol für die Instance, mit der Sie sich verbinden möchten.



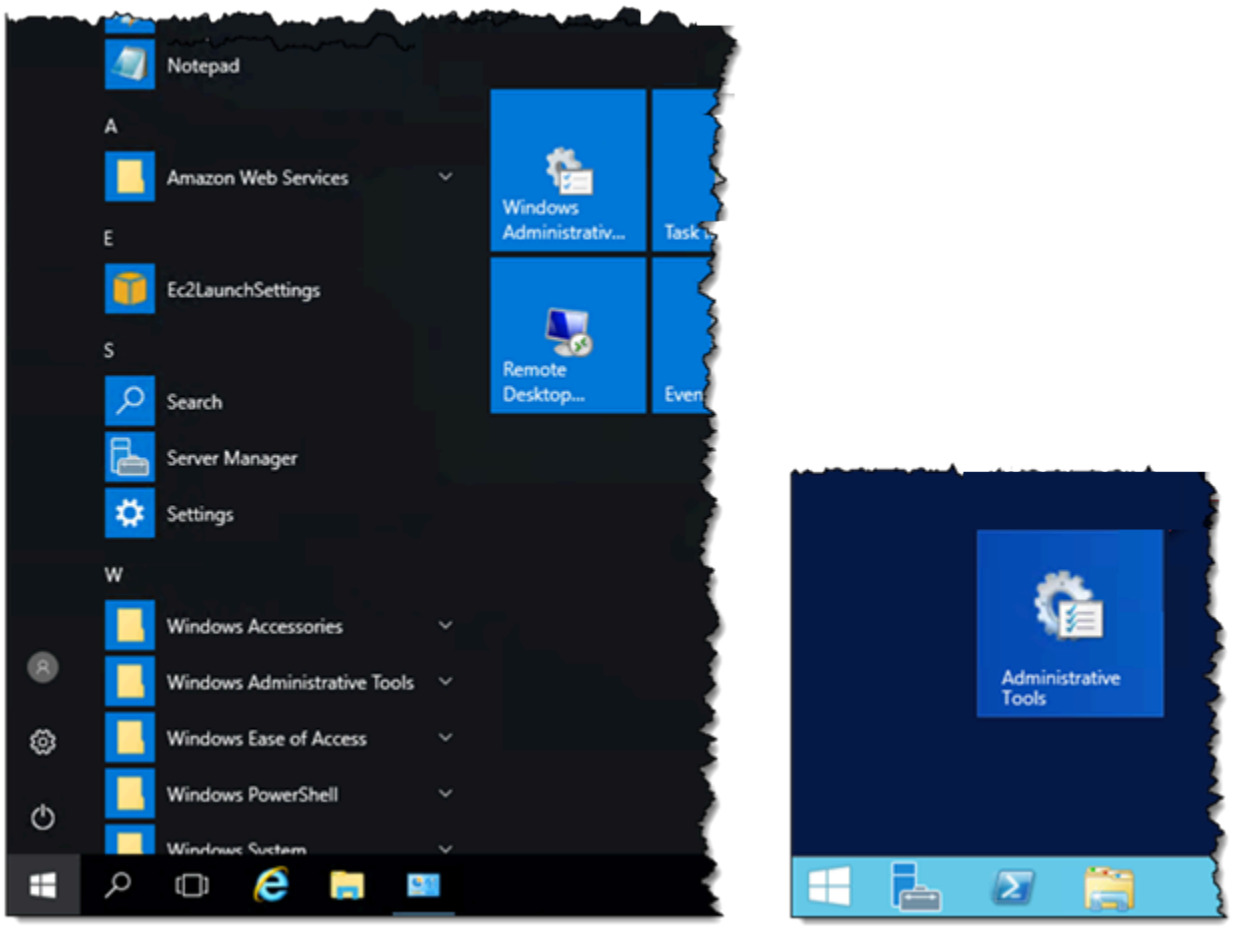
Das browserbasierte RDP-Client-Fenster wird geöffnet, wie im folgenden Beispiel gezeigt:



3. Wählen Sie in der Taskleiste das Windows-Symbol und dann eine der folgenden Optionen:

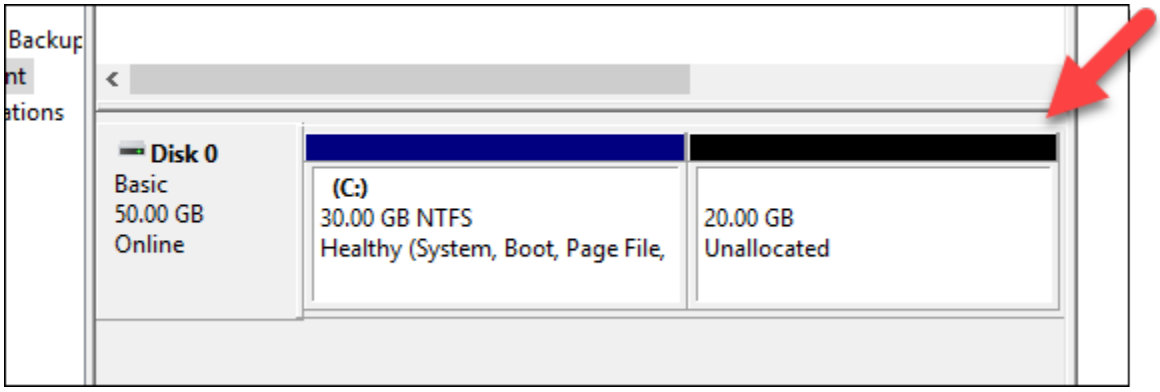
   a. Wählen Sie auf den Windows-Server-2019- und Windows-Server-2016-Instances Start und dann Windows-Administrationswerkzeuge.

b. Wählen Sie auf den Windows Server 2012-Instances Start und dann Administrative Tools (Administrationswerkzeuge).

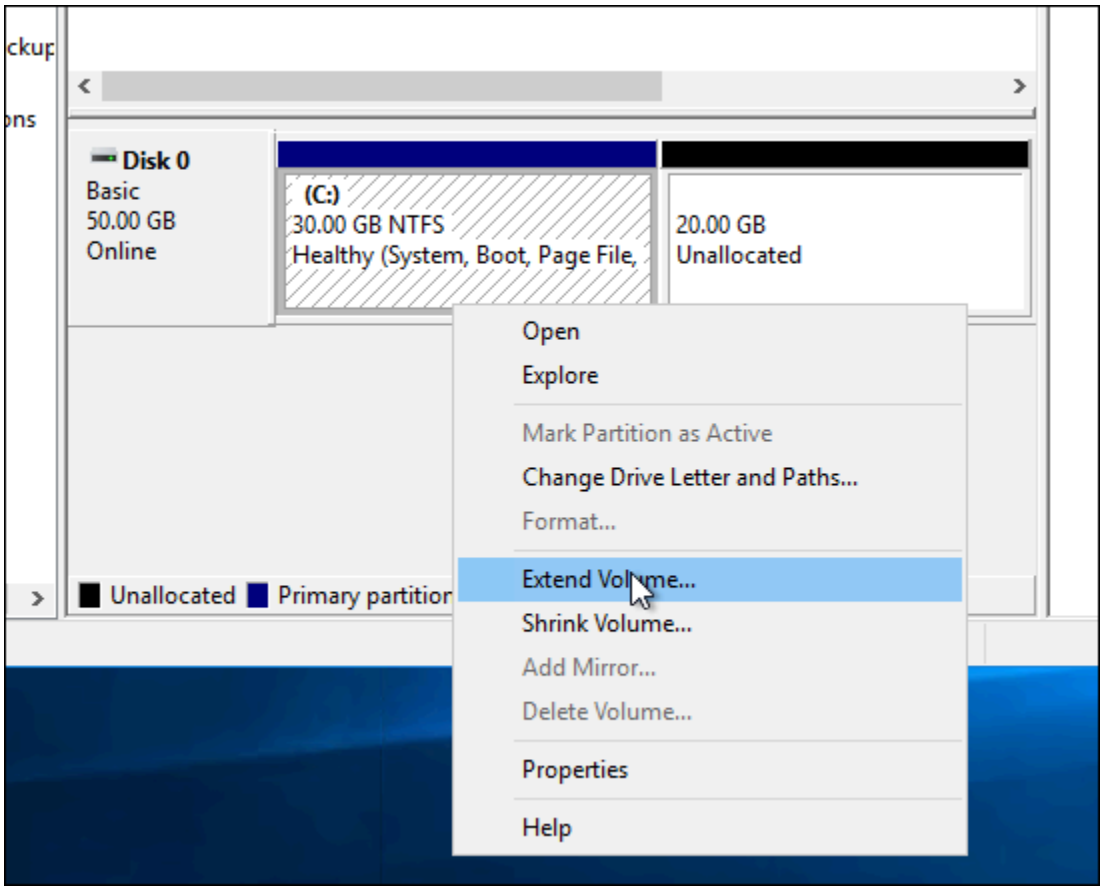


4. Wählen Sie Computer Management (Computerverwaltung).
5. Wählen Sie in der Computerverwaltungskonsole auf der linken Seite Disk Management (Datenträgerverwaltung).
6. Wählen Sie im Menü Actions (Aktionen) die Option Rescan Disks (Datenträger neu scannen).

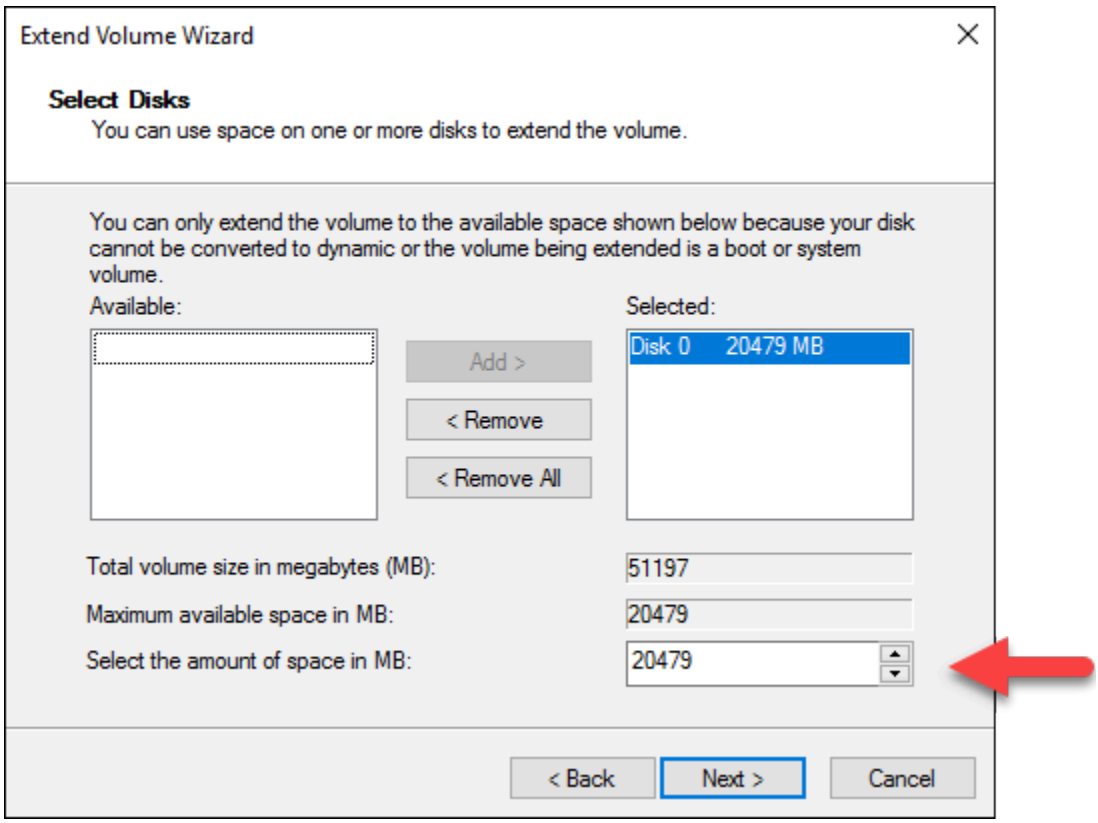
   Möglicherweise wird nicht zugeordneter Speicherplatz angezeigt, der zu einem Datenträger gehört. Erweitern Sie das aktive Volume auf dem Datenträger, um den nicht zugewiesenen Speicherplatz zu nutzen.



7. Klicken Sie mit der rechten Maustaste auf das aktive Volume auf dem Datenträger mit dem nicht zugeordneten Speicherplatz und wählen Sie dann Extend Volume (Volume erweitern).

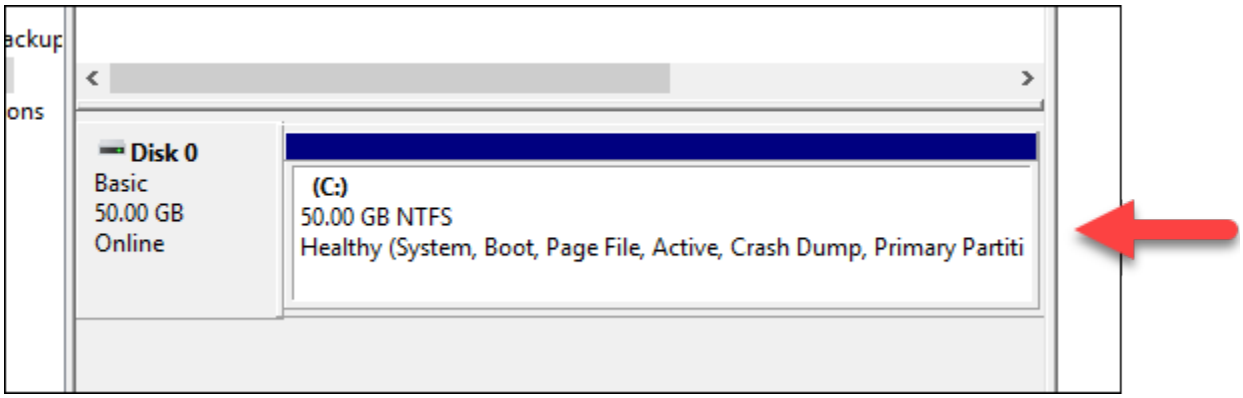


8. Wenn der Assistent für die Erweiterung des Volume geöffnet wird, wählen Sie Next (Weiter).
9. Geben Sie im Feld Select the amount of space in MB (Speicherplatz in MB auswählen) die Anzahl der Megabytes ein, um die Sie das Volume erweitern möchten. Normalerweise wird dieser Wert auf das Maximum des nicht zugewiesenen Speicherplatzes gesetzt. Der Wert, den Sie hier eingeben, ist die Menge an hinzugefügtem Speicherplatz, nicht die endgültige Größe des Volumes.



10. Schließen Sie den Assistenten für die Erweiterung des Volume ab.

    Das aktive Volume wird erweitert, damit der von Ihnen angegebene nicht zugewiesene Speicherplatz verwendet werden kann. Das folgende Beispiel zeigt, wie der gesamte nicht zugewiesene Speicherplatz ausgewählt wird.



Verwenden eines Launch-Skripts zur Konfiguration Ihrer Lightsail-Instance beim Hochfahren

Wenn Sie eine Linux/Unix-basierte Instance erstellen, können Sie ein Skript starten, das beispielsweise Software hinzufügt oder aktualisiert oder Ihre Instance auf andere Weise konfiguriert. Weitere Informationen zum Konfigurieren einer Windows-basierten Instance mit zusätzlichen Daten finden Sie unter Konfigurieren Ihrer neuen Lightsail-Instance mit Windows PowerShell.

> **Note**
>
> Abhängig von dem gewählten Maschinen-Image variiert der Befehl, mit dem Sie Software in Ihre Instance laden. Amazon Linux verwendet `yum`, während Debian und Ubuntu Debian `apt-get` verwenden. WordPress und andere Anwendungs-Images verwenden, `apt-get`, da sie Ubuntu als Betriebssystem verwenden. FreeBSD und openSUSE benötigen eine zusätzliche Benutzerkonfiguration, um benutzerdefinierte Tools wie `freebsd-update` oder `zypper` (openSUSE) zu verwenden.

Beispiel: Konfigurieren eines Ubuntu-Servers zum Installieren von Node.js

Das folgende Beispiel aktualisiert die Paketliste und installiert dann Node.js über den Befehl `apt-get`.

1. Wählen Sie auf der Seite Create an instance (Eine Instance erstellen) Ubuntu auf der Registerkarte OS Only (Nur Betriebssystem).
2. Blättern Sie nach unten und wählen Sie Add launch script (Launch-Skript hinzufügen).
3. Geben Sie Folgendes ein:

```
# update package list
apt-get -y update
# install some of my favorite tools
apt-get install -y nodejs
```

> **Note**
>
> Befehle, die Sie senden, um Ihren Server zu konfigurieren, werden als root ausgeführt, Sie müssen also vor Ihren Befehlen nicht `sudo` angeben.

4. Wählen Sie Create instance (Instance erstellen).

Beispiel: Konfigurieren eines WordPress-Servers, um ein Plugin herunterzuladen und zu installieren

Das folgende Beispiel aktualisiert die Paketliste und lädt dann das BuddyPress-Plugin für WordPress herunter und installiert es.

1. Wählen Sie auf der Seite Create an instance (Eine Instance erstellen) die Option WordPress.
2. Wählen Sie Add launch script (Launch-Script hinzufügen) aus.
3. Geben Sie Folgendes ein:

```
# update package list
apt-get -y update
# download wordpress plugin
wget "https://downloads.wordpress.org/plugin/buddypress.2.7.0.zip"
apt-get -y install unzip
# unzip into wordpress plugin directory
unzip buddypress.2.7.0.zip -d /var/wordpress/plugins
```

4. Wählen Sie Create instance (Instance erstellen).

Konfigurieren Ihrer neuen Lightsail-Instance mit Windows PowerShell oder einem Stapelskript

Beim Erstellen einer Windows-basierten Instance können Sie die Instance mit einem Windows PowerShell-Skript oder einem anderen Stapelskript konfigurieren. Dies ist ein einmaliges Skript, das direkt nach dem Start der Instance ausgeführt wird. In diesem Thema wird die Syntax des Skripts dargestellt und ein Beispiel für die ersten Schritte zur Verfügung gestellt. Wir zeigen Ihnen auch, wie Sie Ihr Skript testen, um zu prüfen, ob es erfolgreich ausgeführt wurde.

Erstellen einer Instance, mit der ein PowerShell-Skript gestartet und ausgeführt wird

Mit dem folgenden Vorgang wird ein Tool namens chocolatey direkt nach dem Start der Instance auf einer neuen Instance installiert.

1. Wählen Sie auf der Lightsail-Startseite Create instance (Instance erstellen).

2. Wählen Sie die AWS-Region und Availability Zone aus, in der Sie Ihre Instance erstellen möchten.
3. Wählen Sie unter Select a platform (Plattform auswählen) die Option Microsoft Windows aus.
4. Wählen Sie Nur OS und danach Windows Server 2019, Windows Server 2016, Windows Server 2012 R2.
5. Wählen Sie Add launch script (Launch-Script hinzufügen) aus.
6. Geben Sie Folgendes ein:

```
<powershell>
iex ((New-Object System.Net.WebClient).DownloadString('https://chocolatey.org/
install.ps1'))
</powershell>
```

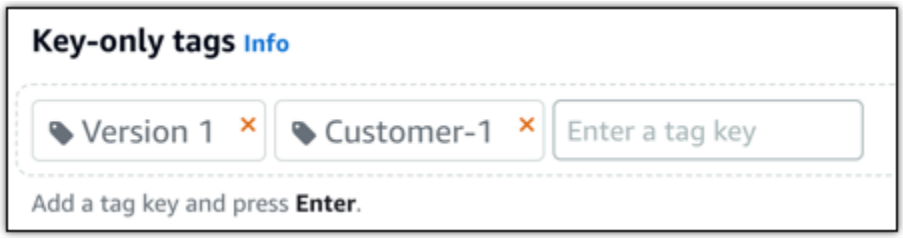
> **Note**
>
> Sie müssen die PowerShell-Skripts immer in `<powershell></powershell>`-Tags setzen. Nicht-PowerShell-Befehle oder Stapelskripts können Sie mit `<script></script>`-Tags oder ganz ohne Tags eingeben.

7. Geben Sie einen Namen für Ihre Instance ein.

   Ressourcennamen:

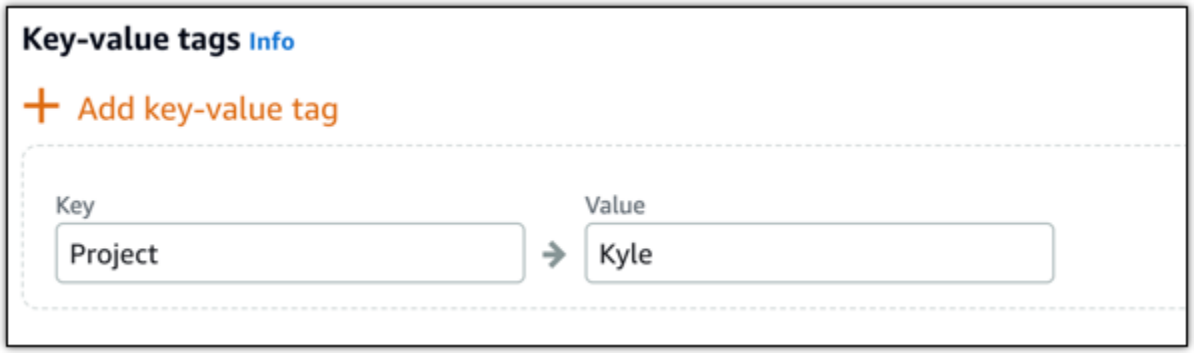
   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.
8. Wählen Sie eine der folgenden Optionen, um Ihrer Instance Tags hinzuzufügen:

   - Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.



- Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

  Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.



> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

9. Wählen Sie Create instance (Instance erstellen).

Überprüfen, ob Ihr Skript erfolgreich ausgeführt wurde

Sie können sich bei Ihrer Instance anmelden, um zu überprüfen, ob das Skript erfolgreich ausgeführt wurde. Es kann bis zu 15 Minuten dauern, bis eine Windows-basierte Instance bereit ist, RDP-Verbindungen zu akzeptieren. Sobald sie bereit ist, melden Sie sich über den browserbasierten RDP-Client an oder konfigurieren Sie einen eigenen RDP-Client. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-basierten Instance.

1. Sobald Sie eine Verbindung mit Ihrer Lightsail-Instance herstellen können, öffnen Sie Eingabeaufforderung (oder Windows Explorer).
2. Geben Sie Folgendes ein, um zum Log-Verzeichnis zu wechseln:

```
cd C:\ProgramData\Amazon\EC2-Windows\Launch\Log
```

> **Note**
>
> In Windows Server 2012 lautet der Befehl `cd C:\Program Files\Amazon\Ec2ConfigService\Logs`.

3. Öffnen Sie `UserdataExecution.log` in einem Texteditor oder geben Sie Folgendes ein: `type UserdataExecution.log`.

   In Ihrer Protokolldatei sollte Folgendes angezeigt werden.

```
2017/10/11 20:32:12Z: <powershell> tag was provided.. running powershell content
2017/10/11 20:32:13Z: Message: The output from user scripts: iex ((New-Object
 System.Net.WebClient).DownloadString('https://chocolatey.org/install.ps1'))

2017/10/11 20:32:13Z: Userdata execution done
```

Bewährte Methoden für die Absicherung von Windows-Server-basierten Instances in Lightsail

In diesem Artikel finden Sie Tipps und Tricks zur Vermeidung von Sicherheitsrisiken bei der Verwendung von Windows Server-Lightsail-Instances.

Informationen zu Lightsail-Passwörtern

Wenn Sie eine Windows Server-basierte Instance erstellen, generiert Lightsail nach dem Zufallsprinzip ein langes Passwort, das schwer zu erraten ist. Dies ist das eindeutige Passwort, das Sie für Ihre neue Instance verwenden. Mithilfe des Standardpassworts können Sie über Remote Desktop (RDP) schnell eine Verbindung mit der Instance herstellen. Sie sind bei Ihrer Lightsail-Instance immer als Administrator angemeldet.

Verwalten Ihres Passworts

Sie können das Passwort für Ihre Windows-Server-basierte Instance ändern. Das ist u. U. praktisch, wenn Sie einen Remote-Desktop-Client für den Zugriff auf die Lightsail-Instance verwenden möchten. Ein von Ihnen generiertes Passwort wird nie von Lightsail gespeichert.

> **Note**
>
> Sie können entweder das von Lightsail generierte Passwort oder ein eigenes, benutzerdefiniertes Passwort mit dem browserbasierten RDP-Client in Lightsail verwenden. Wenn Sie ein benutzerdefiniertes Passwort verwenden, werden Sie bei jeder Anmeldung erneut aufgefordert, Ihr Passwort anzugeben. Wenn Sie schnellen Zugriff auf die Instance benötigen, ist es einfacher, das von Lightsail generierte Standardpasswort mit dem Browser-basierten RDP-Client zu verwenden.

Verwenden Sie den Windows Server-Passwort-Manager, um das Passwort auf sichere Weise zu ändern. Drücken Sie `Ctrl` + `Alt` + `Del` und wählen Sie dann Change a password (Passwort ändern) aus. Notieren Sie Ihr Passwort unbedingt, da Lightsail Ihr Passwort nicht speichert. Informationen zum Abrufen Ihres Kennworts finden Sie unter: Ändern Sie das Administratorkennwort für eine Windows-basierte Instance.

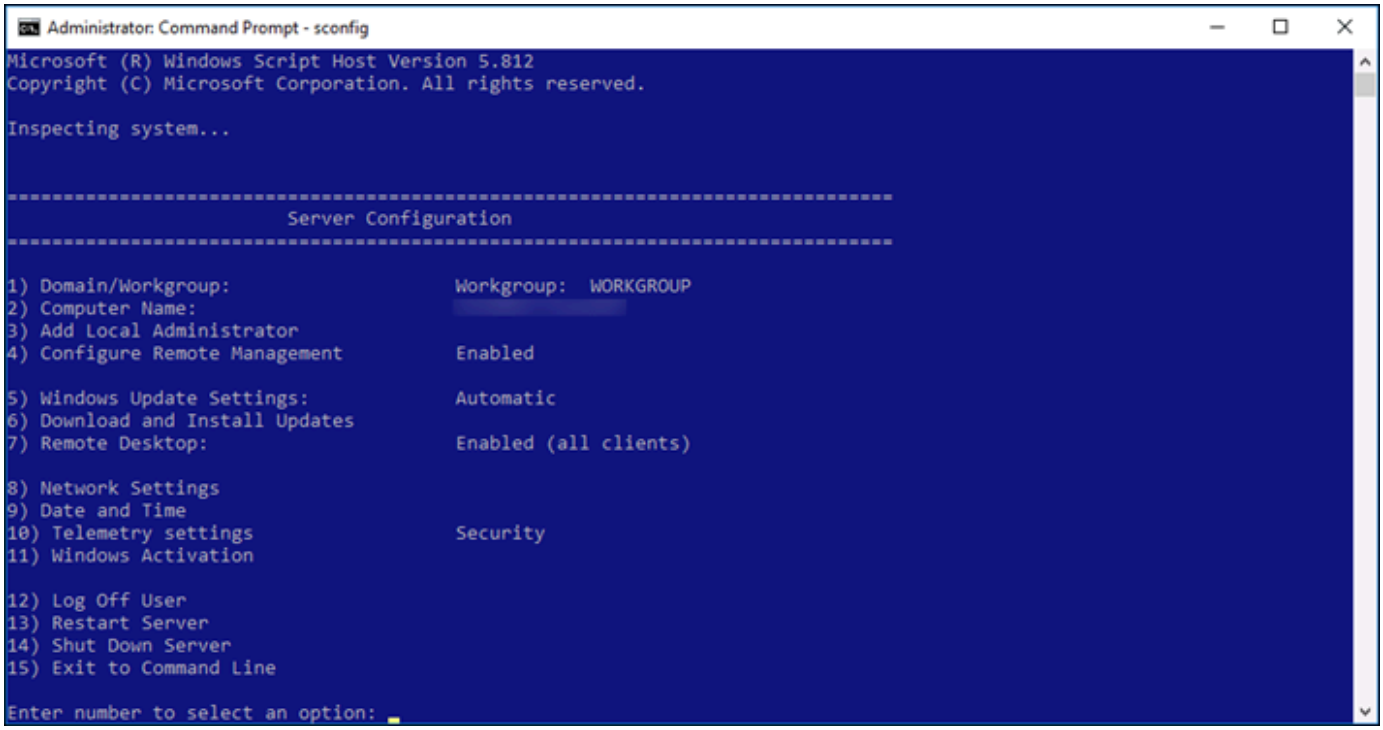
Wenn Sie das eindeutige Standardpasswort ändern möchten, stellen Sie sicher, dass Sie ein sicheres Passwort verwenden. Vermeiden Sie auf Namen oder Wörtern aus dem Wörterbuch basierende Passwörter und Wiederholungen von Zeichenfolgen.

Ausführen von Sicherheits-Patches

Wir empfehlen, die Windows Server-basierte Lightsail-Instance stets mit den neuesten Sicherheits-Patches zu aktualisieren. Stellen Sie sicher, dass der Server konfiguriert ist, um Updates herunterzuladen und zu installieren. Im folgenden Verfahren wird beschrieben, wie Sie dies direkt auf der Windows Server-Lightsail-Instance ausführen.

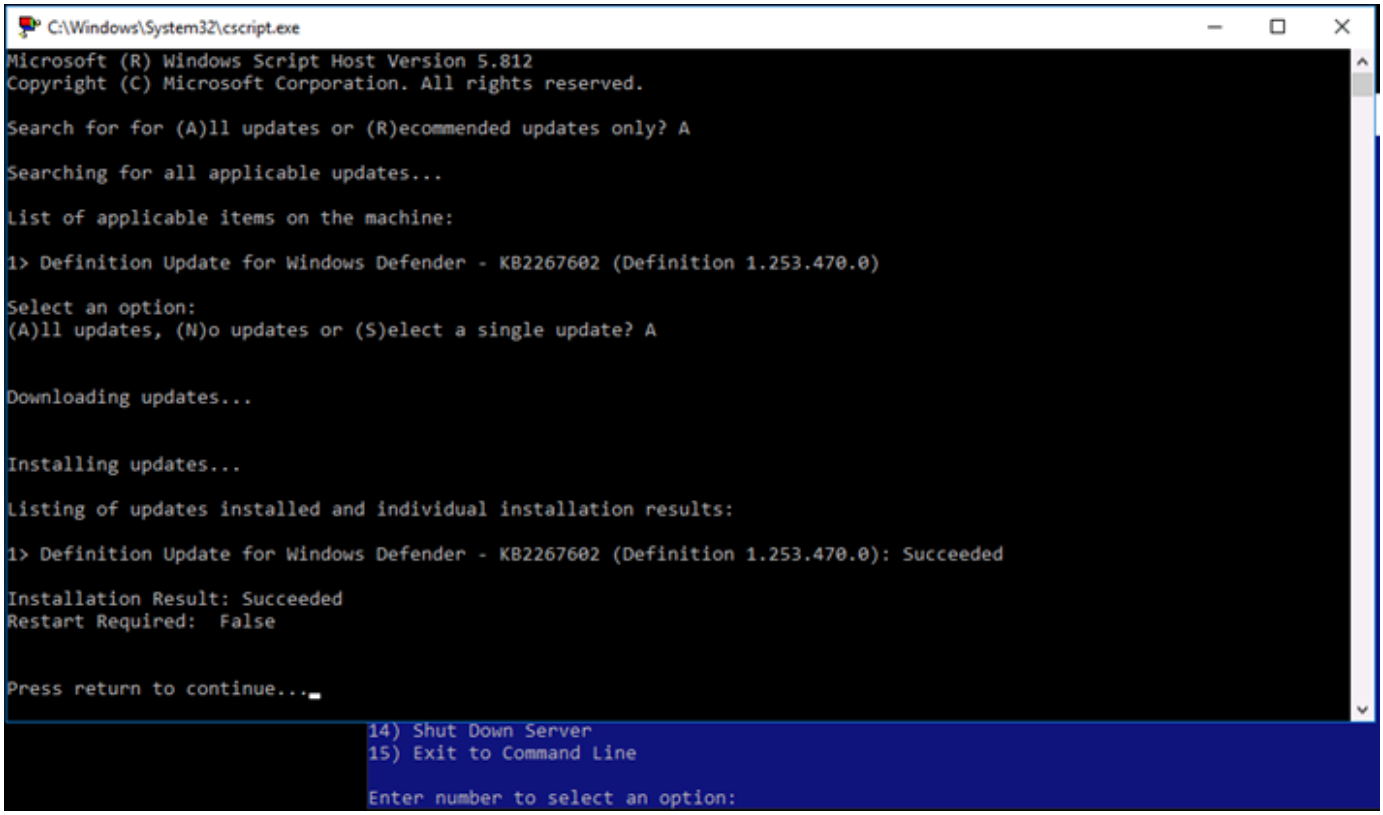
1. Öffnen Sie eine Befehlszeile auf der Windows Server-basierten Instance.
2. Geben Sie `sconfig` ein und drücken Sie auf `Enter`.

   Standardmäßig ist für die Windows Update-Einstellungen (Nummer 5) die Einstellung `Automatic` definiert.



3. Geben Sie zum Herunterladen und Installieren von neuen Updates 6 ein und drücken Sie `Enter`.
4. Geben Sie `A` ein, um im neuen Befehlszeilenfenster nach (A)ll updates ((Alle) Aktualisierungen) zu suchen, und drücken Sie `Enter`.
5. Geben Sie erneut `A` ein, um (A)ll updates ((Alle) Aktualisierungen) zu installieren, und drücken Sie `Enter`.

   Wenn der Vorgang abgeschlossen ist, sehen Sie eine Meldung mit den Installationsergebnissen und ggf. weiteren Anweisungen.



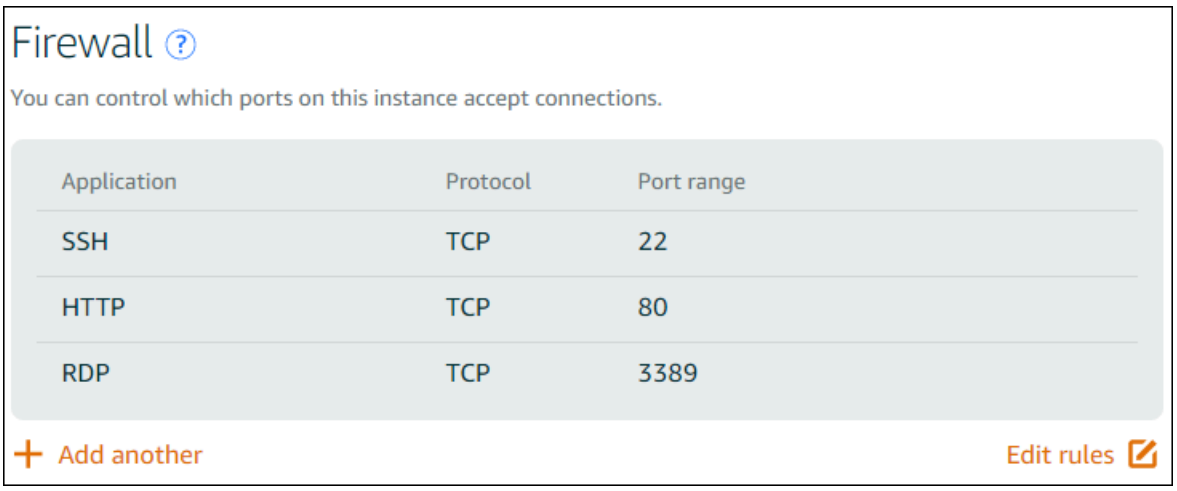
Aktivieren der Richtlinie zur Kontosperrung in Windows Server

Sie können Windows Server konfigurieren, um vorübergehend oder dauerhaft Konten zu deaktivieren, wenn eine bestimmte Anzahl von fehlgeschlagenen Anmeldeversuchen erreicht wird. Sie können beispielsweise den Zugang für jemand sperren, der bei dem Versuch, sich bei der Instance anzumelden, drei falsche Passwörter verwendet hat.

Weitere Informationen finden Sie unter Kontosperrungsrichtlinien in der Windows Server-Dokumentation.

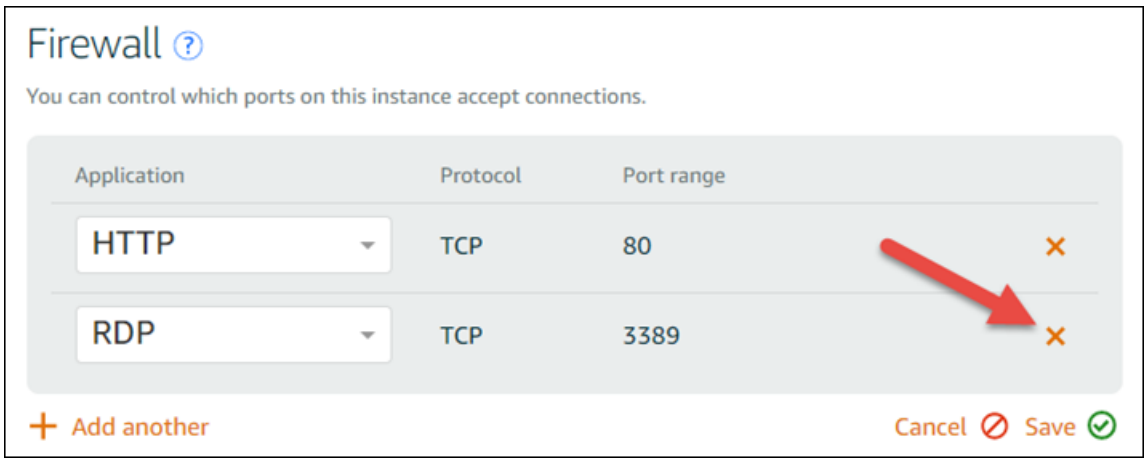
Ports und Firewall-Einstellungen

Standardmäßig öffnen wir die folgenden Ports auf den Windows Server-basierten Instances.



Die Ports, die Sie aktivieren, sind global verfügbar und können nicht durch Quell-IPs beschränkt werden. Zum Einschränken des Zugriffs auf Ihre Instance können Sie diese Ports deaktivieren und nur dann aktivieren, wenn Sie Zugriff auf Ihre Instance benötigen. Das geht so:

1. Suchen Sie die Instance, die Sie in Lightsail verwalten möchten, und wählen Sie Manage (Verwalten) aus.
2. Wählen Sie Networking (Netzwerk).
3. Wählen Sie auf der Seite Networking (Netzwerk) für die Instance die Option Edit rules (Regeln bearbeiten) aus.
4. Löschen Sie die RDP/TCP/3389-Regel, indem Sie auf das orangefarbene "x" daneben klicken.



5. Wählen Sie Save (Speichern).

Referenz zu Lightsail-Firewallregeln

Sie können der Firewall einer Amazon Lightsail-Instance Regeln hinzufügen, die die Rolle der Instance widerspiegeln. Beispielsweise benötigt eine Instance, die als Webserver konfiguriert ist, Firewall-Regeln für eingehenden HTTP- und HTTPS-Zugriff. Eine Datenbank-Instance benötigt Regeln, die den Zugriff für den Datenbanktyp ermöglichen, z. B. den Zugriff über Port 3306 für MySQL. Weitere Informationen zu Firewalls finden Sie unter Instanz-Firewalls in Lightsail.

Dieses Handbuch enthält Beispiele für die Arten von Firewall-Regeln, die Sie einer Instance-Firewall für bestimmte Zugriffsarten hinzufügen können. Die Regeln werden als Anwendungs-, Protokoll-, Port- und Quell-IP-Adresse (z. B. Anwendung – Protokoll – Port – Quell-IP-Adresse) aufgeführt, sofern nicht anders angegeben.

Inhalt

Webserverregeln

Die folgenden eingehenden Regeln erlauben HTTP- und HTTPS-Zugriff.

> **Note**
>
> Für einige Lightsail-Instanzen sind standardmäßig die folgenden Firewallregeln konfiguriert. Weitere Informationen finden Sie unter Firewall und Ports.

HTTP

HTTP – TCP – 80 – alle IP-Adressen

HTTPS

HTTPS – TCP – 443 – alle IP-Adressen

Regeln für die Verbindung mit Ihrer Instance von Ihrem Computer aus

Um eine Verbindung zu Ihrer Instance herzustellen, fügen Sie eine Regel hinzu, die SSH-Zugriff (für Linux-Instanzen) oder RDP-Zugriff (für Windows-Instanzen) zulässt.

> **Note**
>
> Für alle Lightsail-Instanzen ist standardmäßig eine der folgenden Firewallregeln konfiguriert. Weitere Informationen finden Sie unter Firewall und Ports.

SSH

SSH – TCP – 22 – Die öffentliche IP-Adresse Ihres Computers bzw. ein Bereich von IP-Adressen (in CIDR-Block-Notation) in Ihrem lokalen Netzwerk.

RDP

RDP – TCP – 3389 – Die öffentliche IP-Adresse Ihres Computers bzw. ein Bereich von IP-Adressen (in CIDR-Block-Notation) in Ihrem lokalen Netzwerk.

Datenbankserverregeln

Die folgenden eingehenden Regeln sind Beispiele für Regeln, die Sie für den Datenbankzugriff hinzufügen können, je nachdem, auf welcher Art von Datenbank Ihre Instance ausgeführt wird.

SQL Server

Benutzerdefiniert – TCP – 1433 – Die öffentliche IP-Adresse Ihres Computers bzw. ein Bereich von IP-Adressen (in CIDR-Block-Notation) in Ihrem lokalen Netzwerk.

MySQL/Aurora

MySQL/Aurora – TCP – 3306 – Die öffentliche IP-Adresse Ihres Computers bzw. ein Bereich von IP-Adressen (in CIDR-Block-Notation) in Ihrem lokalen Netzwerk.

PostgreSQL

PostgreSQL – TCP – 5432 – Die öffentliche IP-Adresse Ihres Computers bzw. ein Bereich von IP-Adressen (in CIDR-Block-Notation) in Ihrem lokalen Netzwerk.

Oracle-RDS

Oracle-RDS – TCP – 1521 – Die öffentliche IP-Adresse Ihres Computers bzw. ein Bereich von IP-Adressen (in CIDR-Block-Notation) in Ihrem lokalen Netzwerk.

Amazon-Redshift

Benutzerdefiniert – TCP – 5439 – Die öffentliche IP-Adresse Ihres Computers bzw. ein Bereich von IP-Adressen (in CIDR-Block-Notation) in Ihrem lokalen Netzwerk.

DNS-Server-Regeln

Wenn Sie Ihre Instance als DNS-Server eingerichtet haben, müssen Sie sicherstellen, dass TCP- und UDP-Datenverkehr Ihren DNS-Server über Port 53 erreichen kann.

DNS (TCP)

DNS (TCP) – TCP – 53 – Die öffentliche IP-Adresse Ihres Computers bzw. ein Bereich von IP-Adressen (in CIDR-Block-Notation) in Ihrem lokalen Netzwerk.

DNS (UDP)

DNS (UDP) – UDP – 53 – Die öffentliche IP-Adresse Ihres Computers bzw. ein Bereich von IP-Adressen (in CIDR-Block-Notation) in Ihrem lokalen Netzwerk.

SMTP-E-Mail

Zur Aktivierung von SMTP für Ihre Instance müssen Sie die folgende Firewall-Regel konfigurieren.

> **Important**
>
> Nachdem Sie die folgende Regel konfiguriert haben, müssen Sie auch Reverse-DNS für Ihre Instance konfigurieren. Andernfalls kann Ihre E-Mail auf TCP-Port 25 beschränkt sein. Weitere Informationen finden Sie unter Konfigurieren von Reverse-DNS für einen E-Mail-Server.

SMTP

Benutzerdefiniert – TCP – 25 – Die IP-Adressen der Hosts, die mit Ihrer Instance kommunizieren

Instance-Firewalls in Amazon Lightsail

Die Firewall in der Amazon Lightsail-Konsole fungiert als virtuelle Firewall, die den Datenverkehr steuert, der über ihre öffentliche IP-Adresse eine Verbindung zu Ihrer Instance herstellen darf. Jede Instance, die Sie in Lightsail erstellen, verfügt über zwei Firewalls: eine für IPv4-Adressen und eine andere für IPv6-Adressen. Jede Firewall enthält eine Reihe von Regeln, die den Datenverkehr filtern, der in die Instance eingeht. Beide Firewalls sind voneinander unabhängig. Sie müssen daher die Firewall-Regeln für IPv4 und IPv6 getrennt konfigurieren. Bearbeiten Sie die Firewall Ihrer Instance jederzeit, indem Sie Regeln hinzufügen und löschen, um den Datenverkehr zuzulassen oder einzuschränken.

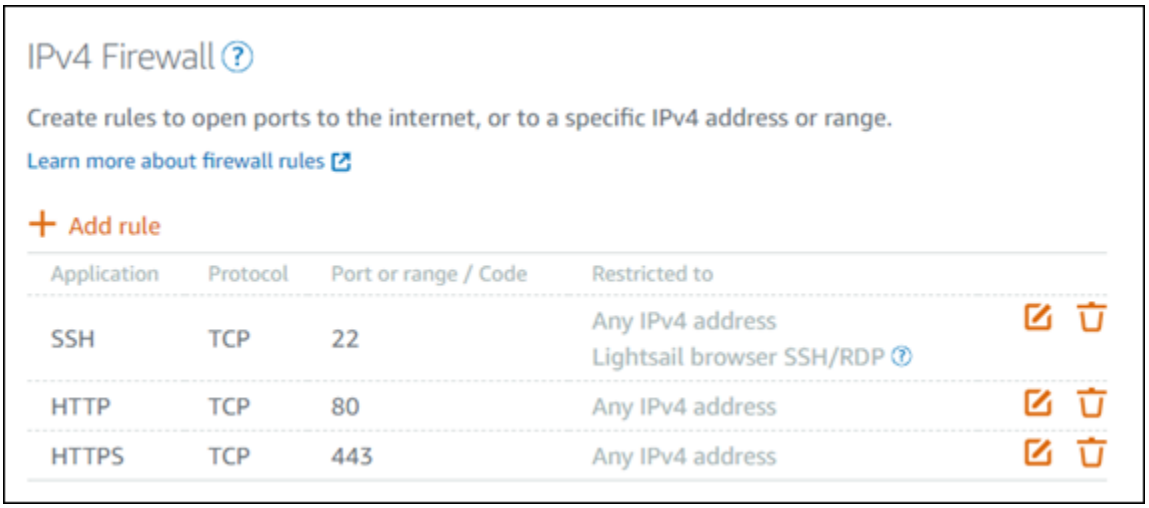
Inhalt

Lightsail-Firewalls

Jede Lightsail-Instance verfügt über zwei Firewalls: eine für IPv4-Adressen und eine andere für IPv6-Adressen. Der gesamte Internetdatenverkehr in und aus Ihrer Lightsail-Instance wird durch die Firewall geleitet. Eine Instance-Firewall steuert den Internetdatenverkehr, der in Ihre Instance fließen darf. Sie steuert jedoch nicht den hinaus fließenden Datenverkehr. Die Firewall erlaubt den gesamten ausgehenden Datenverkehr. Bearbeiten Sie die Firewall Ihrer Instance jederzeit, indem Sie Regeln hinzufügen und löschen, um den Datenverkehr zuzulassen oder einzuschränken. Beachten Sie, dass beide Firewalls voneinander unabhängig sind. Sie müssen daher die Firewallregeln für IPv4 und IPv6 getrennt konfigurieren.

Firewall-Regeln sind stets zulassend, Sie können keine Regeln erstellen, die den Zugriff verweigern. Sie fügen Ihrer Firewall Regeln hinzu, damit der Datenverkehr Ihre Instance erreichen kann. Wenn Sie der Firewall Ihrer Instancer eine Regel hinzufügen, geben Sie, wie im folgenden Beispiel gezeigt,

das zu verwendende Protokoll, den zu öffnenden Port und die IPv4- und IPv6-Adressen an, die eine Verbindung zu Ihrer Instance herstellen dürfen (für IPv4). Sie können auch einen Protokolltyp der Anwendungsebene angeben, bei dem es sich um eine Voreinstellung handelt, die das Protokoll und den Portbereich für Sie auf Grundlage des für Ihre Instance zu verwendenden Diensts angibt.



> **Important**
>
> Firewall-Regeln betreffen nur den Datenverkehr, der durch die öffentliche IP-Adresse einer Instance fließt. Sie wirkt sich nicht auf den Datenverkehr aus, der durch die private IP-Adresse einer Instance fließt, die von Lightsail-Ressourcen in Ihrem Konto AWS-Region, in derselben oder Ressourcen in einer per Peering verbundenen Virtual Private Cloud (VPC) in derselben stammen kann AWS-Region.

Firewall-Regeln und ihre konfigurierbaren Parameter werden in den nächsten Abschnitten dieses Handbuchs erläutert.

Firewall-Regeln erstellen

Erstellen Sie eine Firewall-Regel, damit ein Client eine Verbindung mit Ihrer Instance oder mit einer Anwendung herstellen kann, die auf Ihrer Instance ausgeführt wird. Um beispielsweise allen Webbrowsern zu ermöglichen, sich mit der WordPress Anwendung auf Ihrer Instance zu verbinden, konfigurieren Sie eine Firewallregel, die das Transmission Control Protocol (TCP) über Port 80 von jeder IP-Adresse aus aktiviert. Wenn diese Regel bereits in der Firewall Ihrer Instance konfiguriert ist, können Sie sie löschen, um zu verhindern, dass Webbrowser eine Verbindung mit der WordPress Anwendung auf Ihrer Instance herstellen können.

> **Important**
>
> Sie können die Lightsail-Konsole verwenden, um bis zu 30 Quell-IP-Adressen gleichzeitig hinzuzufügen. Um bis zu 60 IP-Adressen gleichzeitig hinzuzufügen, verwenden Sie die Lightsail-API, AWS Command Line Interface (AWS CLI) oder ein AWS SDK. Dieses Kontingent wird für IPv4-Regeln und IPv6-Regeln getrennt erzwungen. Beispielsweise kann eine Firewall über 60 Regeln für eingehenden IPv4-Datenverkehr und über 60 Regeln für eingehenden IPv6-Datenverkehr verfügen. Wir empfehlen Ihnen, einzelne IP-Adressen in CIDR-Bereichen zu konsolidieren. Weitere Informationen finden Sie im Abschnitt Quell-IP-Adressen angeben in diesem Leitfaden.

Sie können auch einen SSH-Client aktivieren, um eine Verbindung mit Ihrer Instance herzustellen, um administrative Aufgaben auf dem Server auszuführen, indem Sie eine Firewall-Regel konfigurieren, die TCP über Port 22 nur von der IP-Adresse des Computers ermöglicht, der eine Verbindung herstellen muss. In diesem Fall möchten Sie nicht zulassen, dass eine beliebige IP-Adresse eine SSH-Verbindung mit Ihrer Instance herstellen kann, da dies ein Sicherheitsrisiko für Ihre Instance bedeuten könnte.

> **Note**
>
> Die in diesem Abschnitt beschriebenen Firewall-Regelbeispiele können standardmäßig in der Firewall Ihrer Instance vorhanden sein. Weitere Informationen finden Sie unter Standard-Firewall-Regeln weiter unten in diesem Handbuch.

Wenn mehr als eine Regel für einen bestimmten Port vorliegt, wird die toleranteste Regel angewendet. Beispiel: Sie fügen eine Regel hinzu, die den Zugriff auf TCP-Port 22 (SSH) von der IP-Adresse 192.0.2.1 ermöglicht. Anschließend fügen Sie eine weitere Regel hinzu, die den Zugriff auf TCP-Port 22 von allen Benutzern ermöglicht. Infolgedessen hat jeder Benutzer Zugriff auf TCP-Port 22.

Protokolle angeben

Ein Protokoll ist das Format, in dem Daten zwischen zwei Computern übertragen werden. Mit Lightsail können Sie die folgenden Protokolle in einer Firewall-Regel angeben:

- TCP (Transmission Control Protocol) wird hauptsächlich zum Herstellen und Verwalten einer Verbindung zwischen Clients und der auf Ihrer Instance ausgeführten Anwendung verwendet, bis der Datenaustausch abgeschlossen ist. Es handelt sich um ein weit verbreitetes Protokoll, das Sie häufig in den Firewall-Regeln angeben können. TCP garantiert, dass keine übertragenen Daten fehlen und dass alle gesendeten Daten an den beabsichtigten Empfänger weitergeleitet werden. Es ist ideal für Netzwerkanwendungen, die eine hohe Zuverlässigkeit benötigen und für die Übertragungszeit relativ weniger kritisch ist, wie Web-Browsing, Finanztransaktionen und Textnachrichten. Diese Anwendungsfälle verlieren einen deutlich an Wert, wenn Teile der Daten verloren gehen.
- UDP (User Datagram Protocol) wird hauptsächlich für den Aufbau von Verbindungen mit geringer Latenz und verlusttolerierenden Verbindungen zwischen Clients und der auf Ihrer Instance ausgeführten Anwendung verwendet. Es ist ideal für Netzwerkanwendungen, in denen die empfundene Latenz kritisch ist, wie Spiele, Sprach- und Videokommunikation. Bei diesen Anwendungsfällen kann es zu Datenverlust kommen, ohne dass die wahrgenommene Qualität beeinträchtigt wird.
- Internet Control Message Protocol (ICMP) wird in erster Linie zur Diagnose von Problemen bei der Netzwerkkommunikation verwendet, z. B. um festzustellen, ob Daten das beabsichtigte Ziel rechtzeitig erreichen. Es ist ideal für das Ping-Dienstprogramm, mit dem Sie die Geschwindigkeit der Verbindung zwischen Ihrem lokalen Computer und Ihrer Instance testen können. Es gibt an, wie lange Daten benötigen, bis sie Ihre Instance erreichen und zu Ihrem lokalen Computer zurückkehren.

  > **Note**
  >
  > Wenn Sie der IPv6-Firewall Ihrer Instance mithilfe der Lightsail-Konsole eine ICMP-Regel hinzufügen, wird die Regel automatisch für die Verwendung von ICMPv6 konfiguriert. Weitere Informationen finden Sie unter Internet Control Message Protocol für IPv6 in Wikipedia.

- All wird verwendet, um den gesamten Protokolldatenverkehr in Ihre Instance fließen zu lassen. Geben Sie dieses Protokoll an, wenn Sie nicht sicher sind, welches Protokoll angegeben werden soll. Dies schließt alle Internetprotokolle ein, nicht nur die oben angegebenen. Weitere Informationen finden Sie unter Protokollnummern auf der Website der Internet Assigned Numbers Authority.

Angeben von Ports

Ähnlich wie physische Ports auf Ihrem Computer, mit denen Ihr Computer mit Peripheriegeräten wie Tastatur und Maus kommunizieren kann, dienen Netzwerkports als Internet-Kommunikationsendpunkte für Ihre Instance. Wenn ein Computer versucht, eine Verbindung mit Ihrer Instance herzustellen, wird ein Port verfügbar gemacht, über den die Kommunikation hergestellt werden kann.

Die Ports, die Sie in einer Firewall-Regel angeben können, können zwischen 0 und 65535 liegen. Wenn Sie eine Firewall-Regel erstellen, mit der ein Client eine Verbindung mit Ihrer Instance herstellen kann, geben Sie das zu verwendende Protokoll (siehe weiter oben in diesem Handbuch) und die Portnummern an, über die die Verbindung hergestellt werden kann. Sie können auch die IP-Adressen angeben, die mithilfe des Protokolls und des Ports Verbindung herstellen dürfen. Dies wird im nächsten Abschnitt dieses Handbuchs behandelt.

Hier finden Sie einige der häufig verwendeten Ports und die Dienste, die sie verwenden:

- Für die Datenübertragung über File Transfer Protocol (FTP) wird Port 20 verwendet.
- Die Befehlssteuerung über FTP verwendet Port 21.
- Secure Shell (SSH) verwendet Port 22.
- Telnet-Remote-Login-Dienst und unverschlüsselte Textnachrichten verwenden Port 23.
- Das SMTP-E-Mail-Routing (Simple Mail Transfer Protocol) verwendet Port 25.

> **Important**
>
> Um SMTP auf Ihrer Instance zu aktivieren, müssen Sie auch Reverse DNS für Ihre Instance konfigurieren. Andernfalls ist Ihre E-Mail möglicherweise auf TCP-Port 25 beschränkt. Weitere Informationen finden Sie unter Konfigurieren von Reverse-DNS für einen E-Mail-Server auf Ihrer Amazon Lightsail-Instance.

- Der Domain Name System (DNS)-Dienst verwendet Port 53.
- Hypertext Transfer Protocol (HTTP), mit dem Webbrowser eine Verbindung mit Websites herstellen, verwendet Port 80.
- Post Office Protocol (POP3), das von E-Mail-Clients genutzt wird, um E-Mails von einem Server abzurufen, verwendet Port 110.
- Network News Transfer Protocol (NNTP) verwendet Port 119.
- Network Time Protocol (NTP) verwendet Port 123.

- Internet Message Access Protocol (IMAP), das zur Verwaltung digitaler E-Mails genutzt wird, verwendet Port 143.
- SNMP (Simple Network Management Protocol) verwendet Port 161.
- HTTP Secure (HTTPS) HTTP über TLS/SSL, mit dem Webbrowsern eine verschlüsselte Verbindung mit Websites herstellen, verwendet Port 443.

Weitere Informationen finden Sie unter Service Name and Transport Protocol Port Number Registry auf der Website der Internet Assigned Numbers Authority.

Protokolltypen der Anwendungsebene angeben

Sie können einen Protokolltyp der Anwendungsebene angeben, wenn Sie eine Firewall-Regel erstellen. Dabei handelt es sich um Voreinstellungen, die das Protokoll und den Portbereich der Regel auf Grundlage des Diensts angeben, den Sie für Ihre Instance aktivieren möchten. Auf diese Weise müssen Sie nicht nach dem gemeinsamen Protokoll und den Ports suchen, die für Dienste wie SSH, RDP, HTTP und andere verwendet werden sollen. Sie können einfach diese Protokolltypen der Anwendungsebene auswählen, und das Protokoll und der Port werden für Sie angegeben. Wenn Sie Ihr eigenes Protokoll und Ihren eigenen Port angeben möchten, können Sie als Protokolltyp der Anwendungsebene Custom rule (Benutzerdefinierte Regel) auswählen, mit dem Sie diese Parameter steuern können.

> **Note**
>
> Sie können den Protokolltyp der Anwendungsebene nur mithilfe der Lightsail-Konsole angeben. Sie können den Protokolltyp der Anwendungsebene nicht mit der Lightsail-API, AWS Command Line Interface (AWS CLI) oder SDKs angeben.

Die folgenden Protokolltypen auf Anwendungsebene sind in der Lightsail-Konsole verfügbar:

- Custom (Benutzerdefiniert) – wählen Sie diese Option aus, um Ihr eigenes Protokoll und Ihre Ports anzugeben.
- All protocols (Alle Protokolle) – wählen Sie diese Option aus, um alle Protokolle anzugeben und eigene Ports anzugeben.
- All TCP (Alle TCP) – wählen Sie diese Option aus, wenn Sie das TCP-Protokoll verwenden möchten, sich aber nicht sicher sind, welcher Port geöffnet werden soll. Dadurch wird TCP über alle Ports (0-65535) aktiviert.

- All UDP (Alle UDP) – wählen Sie diese Option, aus wenn Sie das UDP-Protokoll verwenden möchten, sich aber nicht sicher sind, welcher Port geöffnet werden soll. Dies ermöglicht UDP über alle Ports (0-65535).
- Alle ICMP – wählen Sie diese Option aus, um alle ICMP-Typen und -Codes anzugeben.
- Custom ICMP (Benutzerdefiniertes ICMP) – wählen Sie diese Option aus, um das ICMP-Protokoll zu verwenden und einen ICMP-Typ und -Code zu definieren. Weitere Informationen zu ICMP-Typen und -Codes finden Sie unter Control-Messages auf Wikipedia.
- DNS – wählen Sie diese Option aus, wenn Sie DNS für Ihre Instance aktivieren möchten. Dies ermöglicht TCP und UDP über Ports 53.
- HTTP – wählen Sie diese Option aus, wenn Sie Webbrowsern die Verbindung zu einer Website ermöglichen möchten, die auf Ihrer Instance gehostet wird. Dadurch wird TCP über Port 80 aktiviert.
- HTTPS – wählen Sie diese Option aus, wenn Sie Webbrowsern ermöglichen möchten, eine verschlüsselte Verbindung mit einer Website herzustellen, die auf Ihrer Instance gehostet wird. Dies ermöglicht TCP über Port 443.
- MySQL/Aurora – wählen Sie diese Option aus, damit ein Client eine Verbindung mit einer MySQL- oder Aurora-Datenbank herstellen kann, die auf Ihrer Instance gehostet wird. Dies ermöglicht TCP über Port 3306.
- Oracle-RDS – wählen Sie diese Option aus, um einem Client die Verbindung mit einer Oracle- oder RDS-Datenbank zu ermöglichen, die auf Ihrer Instance gehostet wird. Dies ermöglicht TCP über Port 1521.
- Ping (ICMP) – wählen Sie diese Option aus, damit Ihre Instance mit dem Ping-Dienstprogramm auf Anfragen antworten kann. Am IPv4-Firewall aktiviert dies ICMP Typ 8 (Echo) und Code -1 (alle Codes). Auf der IPv6-Firewall werden dadurch ICMP Typ 129 (echo reply) und Code 0 aktiviert.
- RDP – wählen Sie diese Option aus, um einem RDP-Client die Verbindung mit Ihrer Instance zu ermöglichen. Dies ermöglicht TCP über Port 3389.
- SSH – wählen Sie diese Option aus, um einem SSH-Client die Verbindung mit Ihrer Instance zu ermöglichen. Dies ermöglicht TCP über Port 22.

Quell-IP-Adressen angeben

Standardmäßig erlauben Firewall-Regeln, dass alle IP-Adressen über das angegebene Protokoll und den angegebenen Port eine Verbindung mit Ihrer Instance herstellen können. Dies ist ideal für Datenverkehr wie Webbrowser über HTTP und HTTPS. Dies stellt jedoch ein Sicherheitsrisiko für

Datenverkehr wie SSH und RDP dar, da Sie nicht zulassen sollten, dass alle IP-Adressen über diese Anwendungen eine Verbindung mit Ihrer Instance herstellen können. Aus diesem Grund können Sie eine Firewall-Regel auf eine IPv4- oder IPv6-Adresse oder einen IP-Adressbereich beschränken.

- Für die IPv4-Firewall - Sie können eine einzelne IPv4-Adresse (z. B. 203.0.113.1) oder einen IPv4-Adressbereich angeben. In der Lightsail-Konsole kann der Bereich mit einem Bindestrich (z. B. 192.0.2.0-192.0.2.255) oder in CIDR-Blockschreibweise (z. B. 192.0.2.0/24) angegeben werden. Weitere Informationen zur CIDR-Block-Notation finden Sie unter Classless Inter-Domain Routing auf Wikipedia.
- Für die IPv6-Firewall - Sie können eine einzelne IPv6-Adresse (z. B. 2001:0db8:85a3:0000:0000:8a2e:0370:7334 oder einen Bereich von IPv6-Adressen angeben. Der IPv6-Bereich kann in der Lightsail-Konsole nur mit CIDR-Blocknotation (z. B. 2001:db8:: /32) angegeben werden. Weitere Informationen zur IPv6 CIDR-Blocknotation finden Sie unter IPv6-CIDR-Blöcke in Wikipedia.

Standardmäßige Lightsail-Firewall-Regeln

Wenn Sie eine neue Instance erstellen, ist die Firewall mit den folgenden Standardregeln vorkonfiguriert, die grundlegenden Zugriff auf Ihre Instance ermöglichen. Die Standardregeln unterscheiden sich je nach Instance-Typ, den Sie erstellen. Diese Regeln werden als Anwendungs-, Protokoll-, Port- und Quell-IP-Adresse aufgelistet (z. B. Anwendung – Protokoll – Port – Quell-IP-Adresse).

AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS, Debian, FreeBSD ,openSUSE und Ubuntu (Basisbetriebssysteme)

SSH – TCP – 22 – alle IP-Adressen

HTTP – TCP – 80 – alle IP-Adressen

WordPress, Ghost, Joomla! PrestaShopund Drupal (CMS-Anwendungen)

SSH – TCP – 22 – alle IP-Adressen

HTTP – TCP – 80 – alle IP-Adressen

HTTPS – TCP – 443 – alle IP-Adressen

cPanel & WHM (CMS-Anwendung)

SSH – TCP – 22 – alle IP-Adressen

DNS (UDP) - UDP - 53 - alle IP-Adressen

DNS (TCP) - TCP - 53 - alle IP-Adressen

HTTP – TCP – 80 – alle IP-Adressen

HTTPS – TCP – 443 – alle IP-Adressen

Benutzerdefiniert – TCP – 2078 – alle IP-Adressen

Benutzerdefiniert – TCP – 2083 – alle IP-Adressen

Benutzerdefiniert – TCP – 2087 – alle IP-Adressen

Benutzerdefiniert – TCP – 2089 – alle IP-Adressen

LAMP, Django, Node.js, MEAN GitLabund Nginx (Entwicklungs-Stacks)

SSH – TCP – 22 – alle IP-Adressen

HTTP – TCP – 80 – alle IP-Adressen

HTTPS – TCP – 443 – alle IP-Adressen

Magento (E-Commerce-Anwendung)

SSH – TCP – 22 – alle IP-Adressen

HTTP – TCP – 80 – alle IP-Adressen

HTTPS – TCP – 443 – alle IP-Adressen

Redmine (Projektmanagementanwendung)

SSH – TCP – 22 – alle IP-Adressen

HTTP – TCP – 80 – alle IP-Adressen

HTTPS – TCP – 443 – alle IP-Adressen

Plesk (Hosting Stack)

SSH – TCP – 22 – alle IP-Adressen

HTTP – TCP – 80 – alle IP-Adressen

HTTPS – TCP – 443 – alle IP-Adressen

Benutzerdefiniert – TCP – 53 – alle IP-Adressen

Benutzerdefiniert – UDP – 53 – alle IP-Adressen

Benutzerdefiniert – TCP – 8443 – alle IP-Adressen

Benutzerdefiniert – TCP – 8447 – alle IP-Adressen

Windows Server 2022, Windows Server 2019 und Windows Server 2016

SSH – TCP – 22 – alle IP-Adressen

HTTP – TCP – 80 – alle IP-Adressen

RDP – TCP – 3389 – alle IP-Adressen

SQL Server Express 2022, SQL Server Express 2019 und SQL Server Express 2016

SSH – TCP – 22 – alle IP-Adressen

HTTP – TCP – 80 – alle IP-Adressen

RDP – TCP – 3389 – alle IP-Adressen

Weitere Informationen zu Firewalls

Im Folgenden finden Sie einige Artikel, die Sie bei der Verwaltung von Firewalls in Lightsail unterstützen.

- Hinzufügen und Bearbeiten von Instance-Firewall-Regeln
- Referenz zu Firewall-Regeln

Hinzufügen und Bearbeiten von Instance-Firewall-Regeln in Amazon Lightsail

Sie können der IPv4- und IPv6-Firewall für Ihre Amazon Lightsail-Instance Regeln hinzufügen, um den Datenverkehr zu steuern, der eine Verbindung dazu herstellen darf. Wenn Sie eine Firewall-Regel hinzufügen, können Sie den Protokolltyp der Anwendungsebene, das Protokoll, die Ports und die Quellen IPv4 und IPv6 angeben, die eine Verbindung zu Ihrer Instance herstellen dürfen. Weitere Informationen zu Firewalls finden Sie unter Firewall und Ports.

Inhalt

- Hinzufügen und Bearbeiten von Firewall-Regeln
- Löschen von Instance-Firewall-Regeln
- Weitere Informationen zu Firewalls

Hinzufügen und Bearbeiten von Instance-Firewall-Regeln

Führen Sie die folgenden Schritte aus, um Firewall-Regeln in der Lightsail-Konsole hinzuzufügen oder zu bearbeiten.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Instances.
3. Wählen Sie den Namen der Instance aus, für die Sie eine Firewall-Regel hinzufügen oder bearbeiten möchten.
4. Wählen Sie auf der Verwaltungsseite Ihrer Instance die Registerkarte Networking (Netzwerk) aus.

   Auf der Registerkarte Networking (Netzwerk) werden die öffentlichen und privaten IP-Adressen Ihrer Instance sowie die konfigurierten IPv4- und IPv6- Firewalls für Ihre Instance angezeigt.

   > **Note**
   >
   > Die IPv6-Firewall wird nur angezeigt, wenn Sie IPv6 für die Instance aktiviert haben. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren von IPv6.

5. Führen Sie einen der folgenden Schritte aus, je nachdem, ob es sich bei der Quell-IP für die Regel um eine IPv4- oder IPv6-Adresse handelt:

   - Um eine IPv4-Firewall-Regel hinzuzufügen, scrollen Sie nach unten zum Abschnitt IPv4-Firewall der Seite und wählen Sie Add rule (Regel hinzufügen).
   - Um eine IPv6-Firewall-Regel hinzuzufügen, scrollen Sie nach unten zum Abschnitt IPv6-Firewall der Seite und wählen Sie Add rule (Regel hinzufügen).

   Sie können neben einer vorhandenen Regel auch Edit (Bearbeiten) (Bleistiftsymbol) auswählen, um sie zu bearbeiten.
6. Wählen Sie im Dropdown-Menü Application (Anwendung) einen Protokolltyp der Anwendungsebene aus.

Wenn Sie einen Protokolltyp der Anwendungsebene auswählen, werden ein Satz von Protokoll- und Port-Voreinstellungen für Sie angegeben. Beispielwerte: Custom (Benutzerdefiniert), All TCP (Alle TCP), All UDP (Alle UDP), Custom ICMP (Benutzerdefiniertes ICMP), SSH und RDP.

Je nach ausgewähltem Protokolltyp der Anwendungsebene können Sie die folgenden optionalen Einstellungen konfigurieren:

- (Optional) Wenn Sie die Option Custom (Benutzerdefiniert) auswählen, können Sie im Dropdown-Menü Protocol (Protokoll) einen Wert auswählen. Die verfügbaren Protokollwerte: TCP und UDP.

  Sie können auch eine einzelne Portnummer oder einen Portnummernbereich (z. B. 7000-8000) in das Feld Port eingeben.
- (Optional) Wenn Sie die Option Custom ICMP (Benutzerdefiniertes ICMP) auswählen, können Sie im Feld Type (Typ) einen ICMP-Typ und im Feld Code einen ICMP-Code angeben. Weitere Informationen zu ICMP-Typen und -Codes finden Sie unter Control-Messages auf Wikipedia.

  > **Note**
  >
  > Wenn Sie der IPv6-Firewall Ihrer Instance mithilfe der Lightsail-Konsole eine ICMP-Regel hinzufügen, wird die Regel automatisch für die Verwendung von ICMPv6 konfiguriert. Weitere Informationen finden Sie unterInternet Control Nachrichtenprotokoll für IPv6inWikipedia.
- (Optional) Wählen Sie Restrict to IP address (Auf IP-Adresse beschränken), um den Zugriff auf das angegebene Protokoll und den Port auf eine bestimmte IP-Adresse oder einen IP-Adressbereich zu beschränken. Lassen Sie diese Option deaktiviert, um alle IP-Adressen für das angegebene Protokoll und den angegebenen Port zuzulassen.

  Sie können eine einzelne IPv4-Adresse (z. B. `203.0.113.1`) oder einen IPv4-Adressbereich eingeben. Der Bereich kann mit einem Bindestrich (z. B. `192.0.2.0-192.0.2.255`) oder in CIDR-Blocknotation (z. B. `192.0.2.0/24`) angegeben werden. Weitere Informationen zur CIDR-Block-Notation finden Sie unter Classless Inter-Domain Routing auf Wikipedia.
- (Optional) Wenn Sie als Protokolltyp der Anwendungsebene SSH oder RDP und dann Restrict to IP address (Auf IP-Adresse einschränken) auswählen, können Sie Allow Lightsail browser SSH/RDP (-Browser SSH/RDP zulassen) auswählen, um die Verbindung mit Ihrer

Instance über die browserbasierten SSH- und RDP-Clients zu ermöglichen, die in der Lightsail-Konsole verfügbar sind. Lassen Sie diese Option deaktiviert, um den Zugriff über diese browserbasierten Clients zu blockieren.

7. Wählen Sie Create (Erstellen) aus, um die Regel der Firewall hinzuzufügen.

   Die Firewall-Regel wird nach wenigen Augenblicken hinzugefügt.

Löschen von Instance-Firewall-Regeln

Führen Sie die folgenden Schritte aus, um Instance-Firewall-Regel in der Lightsail-Konsole zu löschen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Instances.
3. Wählen Sie den Namen der Instance, für die Sie eine Firewall-Regel löschen möchten.
4. Wählen Sie auf der Verwaltungsseite Ihrer Instance die Registerkarte Networking (Netzwerk) aus.
5. Führen Sie einen der folgenden Schritte aus, je nachdem, ob es sich bei der Quell-IP für die Regel um eine IPv4- oder IPv6-Adresse handelt:

   - Scrollen Sie nach unten zum Abschnitt IPv4-Firewall der Seite und wählen Sie Delete (Löschen) (das Papierkorbsymbol) neben einer vorhandenen Regel aus, um eine IPv4-Firewall-Regel zu löschen.
   - Scrollen Sie nach unten zum Abschnitt IPv6-Firewall der Seite und wählen Sie Delete (Löschen) (das Papierkorbsymbol) neben einer vorhandenen Regel aus, um eine IPv6-Firewall-Regel zu löschen.

> **Important**
>
> Firewall-Regeln betreffen nur den Datenverkehr, der durch die öffentliche IP-Adresse einer Instance fließt. Dies wirkt sich nicht auf den Datenverkehr aus, der durch die private IP-Adresse einer Instance fließt, die aus Lightsail-Ressourcen in Ihrem Konto, in derselben AWS-Region oder Ressourcen in einer peered Virtual Private Cloud (VPC) in derselben AWS-Region stammen kann. Wenn Sie beispielsweise die SSH-Regel (TCP-Port 22) aus der Instance-Firewall löschen, können andere Instances im selben

Lightsail-Konto und in derselben AWS-Region weiterhin eine Verbindung mit ihr über SSH herstellen, indem Sie die private IP-Adresse der Instance angeben.

Die Firewall-Regel wird nach wenigen Augenblicken gelöscht.

Weitere Informationen zu Firewalls

Im Folgenden finden Sie einige Artikel, die Sie bei der Verwaltung von Firewalls in Lightsail unterstützen.

- Firewall und Ports
- Referenz zu Firewall-Regeln

Instance Metadata Service (IMDS) und Benutzerdaten in Lightsail

Instance-Metadaten sind Daten über eine Instance, mit denen Sie die ausgeführte Instance konfigurieren und verwalten können. Instance-Metadaten sind in Kategorien unterteilt, z. B. Hostname, Ereignisse und Sicherheitsgruppen. Sie können Instance-Metadaten auch verwenden, um auf Benutzerdaten zuzugreifen, die Sie beim Start Ihrer Instance angegeben haben. Sie können beispielsweise Parameter für die Konfiguration Ihrer Instance angeben oder ein einfaches Skript einbinden. Instances können außerdem dynamische Daten enthalten, z. B. ein Instance-Identitätsdokument, das beim Start der Instance generiert wird.

Important

Sie können nur innerhalb der Instance selbst auf Instance-Metadaten und Benutzerdaten zugreifen. Die Daten sind nicht durch Authentifizierungs- oder kryptografische Verfahren geschützt. Jeder, der direkten Zugriff auf die Instance hat, und möglicherweise auch jede Software, die auf der Instance läuft, kann deren Metadaten einsehen. Daher sollten Sie sensible Daten wie Passwörter oder langlebige Verschlüsselungscodes nicht als Benutzerdaten speichern.

Verwenden des Instance-Metadaten-Services

Sie können mit einer der folgenden Methoden auf Instance-Metadaten aus einer laufenden Instance in Lightsail zugreifen:

- Instance-Metadatenservice Version 1 (IMDSv1) – Ein Anfrage/Antwort-Verfahren
- Instance-Metadatenservice Version 2 (IMDSv2) – Ein sitzungsorientiertes Verfahren

> **Important**
>
> Nicht alle Instance-Vorlagen in Lightsail unterstützen IMDSv2. Verwenden Sie die `MetadataNoToken`-Instance-Metrik, um die Anzahl der Aufrufe an den Instance-Metadaten-Service, die IMDSv1 verwenden, zu verfolgen. Weitere Informationen finden Sie unter Anzeigen von Instance-Metriken.

Weitere Informationen über die Verwendung von IMDS finden Sie unter Konfiguration des Instance Metadata Service (IMDS).

Zusätzliche IMDS-Dokumentation

Die folgende IMDS-Dokumentation ist im Benutzerhandbuch der Amazon Elastic Compute Cloud für Linux-Instances und im Benutzerhandbuch der Amazon Elastic Compute Cloud für Windows-Instances verfügbar:

> **Note**
>
> In Amazon EC2 werden Instance-Vorlagen als Amazon Machine Images (AMI) bezeichnet.

- Für Linux-Instances:
  - Konfigurieren der Instance-Metadaten-Optionen
  - Abrufen von Instance-Metadaten
  - Arbeiten mit Instance-Benutzerdaten
  - Abrufen von dynamischen Daten
  - Instance-Metadatenkategorien
  - Beispiel: AMI-Startindexwert

  - Instance-Identitätsdokumente
- Für Windows-Instances:
  - Konfigurieren der Instance-Metadaten-Optionen
  - Abrufen von Instance-Metadaten
  - Arbeiten mit Instance-Benutzerdaten
  - Abrufen von dynamischen Daten
  - Instance-Metadatenkategorien
  - Beispiel: AMI-Startindexwert
  - Instance-Identitätsdokumente

Konfigurieren des Instance Metadata Service (IMDS) in Lightsail

Sie können mit einer der folgenden Methoden auf Instance-Metadaten aus einer laufenden Instance zugreifen:

- Instance-Metadatenservice Version 1 (IMDSv1) – Ein Anfrage/Antwort-Verfahren
- Instance-Metadatenservice Version 2 (IMDSv2) – Ein sitzungsorientiertes Verfahren

> **Important**
>
> Nicht alle Instance-Vorlagen in Lightsail unterstützen IMDSv2. Verwenden Sie die `MetadataNoToken`-Instance-Metrik, um die Anzahl der Aufrufe an den Instance-Metadaten-Service, die IMDSv1 verwenden, zu verfolgen. Weitere Informationen finden Sie unter Anzeigen von Instance-Metriken.

Standardmäßig können Sie entweder IMDSv1 oder IMDSv2 oder beides verwenden. Der Instance Metadata Service unterscheidet zwischen IMDSv1- und IMDSv2-Anfragen, je nachdem, ob bei einer bestimmten Anfrage entweder der `PUT`- oder `GET`-Header (der für IMDSv2 eindeutig ist) vorhanden ist. Weitere Informationen finden Sie unter Erweitern Sie den EC2-Instance-Metadata-Service, um Abwehr von offenen Firewalls, Reverse-Proxys und SSRF-Schwachstellen mit Verbesserungen an EC2-Instance-Metadata-Service.

Sie können den Instance-Metadaten-Service auf jeder Instance so konfigurieren, dass lokaler Code oder Benutzer IMDSv2 verwenden müssen. Wenn Sie angeben, dass IMDSv2 verwendet werden

muss, funktioniert IMDSv1 nicht mehr. Weitere Informationen finden Sie unter Konfigurieren des Instance Metadata Service im Benutzerhandbuch für Amazon Elastic Compute Cloud für Linux-Instances.

Informationen zum Abrufen von Instance-Metadaten finden Sie unter Instance-Metadaten abrufen im Benutzerhandbuch für Amazon Elastic Compute Cloud für Linux-Instances.

> **Note**
>
> In den Beispielen in diesem Abschnitt wird die IPv4-Adresse des Instance-Metadaten-Service verwendet: `169.254.169.254`. Wenn Sie Instance-Metadaten für Instances über die IPv6-Adresse abrufen, stellen Sie sicher, dass Sie stattdessen die IPv6-Adresse aktivieren und verwenden: `fd00:ec2::254`. Die IPv6-Adresse des Instance-Metadatendienstes ist mit IMDSv2-Befehlen kompatibel.

Funktionsweise von Instance-Metadatenservice Version 2

IMDSv2 verwendet sitzungsorientierte Anfragen. Bei sitzungsorientierten Anforderungen erstellen Sie ein Sitzungs-Token, das die Sitzungsdauer definiert, die mindestens eine Sekunde und maximal sechs Stunden betragen kann. Während der angegebenen Dauer können Sie dasselbe Sitzungs-Token für nachfolgende Anfragen verwenden. Nach Ablauf der angegebenen Dauer müssen Sie ein neues Sitzungs-Token erstellen, das Sie für zukünftige Anfragen verwenden können.

> **Important**
>
> Lightsail-Instances, die über Amazon Linux 2023 gestartet wurden, sind standardmäßig mit IMDSv2 konfiguriert.

Die folgenden Beispiele verwenden ein Linux- und PowerShell-Shell-Skript und IMDSv2, um die Metadatenelemente der Top-Level-Instance abzurufen. Diese Beispiele machen Folgendes:

- Erstellen ein Sitzungs-Token mit einer Dauer von sechs Stunden (21.600 Sekunden) unter Verwendung der PUT-Anfrage
- Speichern den Sitzungs-Token-Header in einer Variablen namens `TOKEN` (unter Linux) oder `token` (unter Windows)
- Fordern die Top-Level-Metadatenelemente über das Token an

Führen Sie zunächst die folgenden Befehle aus:

- Unter Linux:
  - Generieren Sie zuerst ein Token mit dem folgenden Befehl.

    ```
    [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
    ```

  - Verwenden Sie dann das Token, um mit dem folgenden Befehl Top-Level-Metadatenelemente zu generieren.

    ```
    [ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
    ```

- Unter Windows:
  - Generieren Sie zuerst ein Token mit dem folgenden Befehl.

    ```
    PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
    ```

  - Verwenden Sie dann das Token, um mit dem folgenden Befehl Top-Level-Metadatenelemente zu generieren.

    ```
    PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
     GET -Uri http://169.254.169.254/latest/meta-data/
    ```

Nachdem Sie ein Token erstellt haben, können Sie es bis zum Ablauf wiederverwenden. In den folgenden Beispielen ruft jeder Befehl die ID des Blueprints (Amazon Machine Image (AMI)) ab, der zum Starten der Instance verwendet wird. Das Token aus dem vorherigen Beispiel wird wiederverwendet. Es ist in `$TOKEN` (unter Linux) oder `$token` (unter Windows) gespeichert.

- Unter Linux:

  ```
  [ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/ami-id
  ```

- Unter Windows:

  ```
  PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
  ```

```
-Method GET -uri http://169.254.169.254/latest/meta-data/ami-id
```

Wenn Sie IMDSv2 zum Anfordern von Instance-Metadaten verwenden, muss die Anforderung Folgendes enthalten:

- Eine **PUT**-Anfrage – Verwenden Sie eine PUT-Anfrage, um eine Sitzung mit dem Instance Metadata Service zu starten. Die PUT-Anfrage gibt ein Token zurück, das in nachfolgenden GET-Anfragen an den Instance-Metadaten-Service enthalten sein muss. Das Token wird für den Zugriff auf Metadaten mit IMDSv2 benötigt.
- Das Token – Nehmen Sie das Token in alle GET-Anfragen an den Instance Metadata Service auf. Wenn die Token-Verwendung auf `required` festgelegt ist, erhalten Anfragen ohne gültiges Token oder mit abgelaufenem Token einen `401 - Unauthorized`-HTTP-Fehlercode. Informationen zum Ändern der Token-Nutzungsanforderung finden Sie unter Ändern der Instance-Metadatenoptionen in der AWS CLI-Befehlsreferenz.
  - Das Token ist ein Instance-bezogener Schlüssel. Das Token ist in anderen Instances nicht gültig und wird abgelehnt, wenn Sie versuchen, es außerhalb der Instance zu verwenden, in der es erzeugt wurde.
  - Die PUT-Anfrage muss einen Header enthalten, der die Time To Live (TTL) für das Token in Sekunden angibt. Die TTL kann auf maximal sechs Stunden (21.600 Sekunden) festgelegt werden. Das Token stellt eine logische Sitzung dar. Die TTL gibt die Gültigkeitsdauer des Token und damit die Dauer der Sitzung an.
  - Nachdem ein Token abgelaufen ist, müssen Sie eine neue Sitzung mit einer anderen PUT-Anfrage erstellen, um auf die Instance-Metadaten zuzugreifen.
  - Sie können auswählen, ob Sie ein Token wiederverwenden oder bei jeder Anforderung einen neues Token erstellen möchten. Für eine kleine Anzahl von Anfragen kann es einfacher sein, bei jedem Zugriff auf den Instance-Metadaten-Service ein Token zu generieren und sofort zu verwenden. Aus Effizienzgründen können Sie jedoch eine längere Dauer für das Token festlegen und es wiederverwenden, anstatt jedes Mal eine PUT-Anfrage stellen zu müssen, wenn Sie Instance-Metadaten anfordern müssen. Es gibt keine praktische Begrenzung der Anzahl der gleichzeitigen Tokens, die jeweils eine eigene Sitzung darstellen. IMDSv2 ist jedoch immer noch durch die normale Metadatenverbindung der Instance und die Drosselungsgrenzen eingeschränkt. Weitere Informationen dazu finden Sie unter Abfrage-Drosselung im Benutzerhandbuch für Amazon Elastic Compute Cloud für Linux-Instances.

In PUT-Instance-Metadatenanfragen sind HTTP `GET`- und `HEAD`-Methoden zulässig. -Anfragen werden abgelehnt, wenn sie einen `X-Forwarded-For`-Header enthalten.

Standardmäßig hat die Antwort auf PUT-Anfragen auf IP-Protokollebene ein Antworthop-Limit (Time To Live) von `1`. Sie können das Hop-Limit mit dem Befehl `update-instance-metadata-options` anpassen, wenn Sie ein größeres benötigen. Beispielsweise benötigen Sie möglicherweise eine größeres Hop-Limit für die Abwärtskompatibilität mit Container-Services, die auf der Instance ausgeführt werden. Weitere Informationen finden Sie unter update-instance-metadata-options in AWS CLI-Befehlsreferenz.

Übergang zur Verwendung von Instance-Metadatenservice Version 2

Die Verwendung von Instance Metadata Service Version 2 (IMDSv2) ist optional. Instance-Metadatenservice Version 1 (IMDSv1) wird weiterhin auf unbestimmte Zeit unterstützt. Wenn Sie sich für die Migration zu IMDSv2 entscheiden, empfehlen wir Ihnen, die folgenden Tools und Wege zu verwenden.

Tools zur Unterstützung beim Wechsel zu IMDSv2

Wenn Ihre Software IMDSv1 verwendet, verwenden Sie die folgenden Tools, um Ihre Software für die Verwendung von IMDSv2 neu zu konfigurieren.

- AWS-Software: Die neuesten Versionen der AWS-SDKs und AWS CLI unterstützen IMDSv2. Um IMDSv2 zu verwenden, stellen Sie sicher, dass Ihre Instances über die neuesten Versionen der AWS-SDKs und die AWS CLI verfügen. Informationen zum Aktualisieren der AWS CLI finden Sie unter Installieren, Aktualisieren und Deinstallieren von AWS CLI im AWS Command Line Interface-Benutzerhandbuch. Alle Amazon-Linux-2-Softwarepakete unterstützen IMDSv2.
- Instance-Metrik: IMDSv2 nutzt Token-gestützte Sitzungen, während IMDSv1 das nicht tut. Die `MetadataNoToken`-Instance-Metrik erfasst die Anzahl der Aufrufe des Instance-Metadatendienstes, die IMDSv1 verwenden. Indem Sie diese Metrik bis zum Wert Null nachverfolgen, können Sie feststellen, ob und wann Ihre Software auf IMDSv2 upgegradet wurde. Weitere Informationen finden Sie unter Anzeigen von Instance-Metriken in Amazon Lightsail.
- Aktualisierungen an Lightsail-API-Operationen und AWS CLI-Befehlen: Für bestehende Instances können Sie den AWS CLI-Befehl update-instance-metadata-options (oder die API-Operation UpdateInstanceMetadataOptions) verwenden, um die Verwendung von IMDSv2 zu verlangen. Nachfolgend finden Sie einen Beispielbefehl. Stellen Sie sicher, dass Sie *`InstanceName`* durch den Namen Ihrer Instance und *`RegionName`* durch den Namen der AWS-Region ersetzen, in der sich Ihre Instance befindet.

```
aws lightsail update-instance-metadata-options --region RegionName --instance-
name InstanceName --http-tokens required
```

Empfohlener Weg zur Erzwingung des IMDSv2-Zugriffs

Bei Verwendung der oben genannten Tools empfehlen wir Ihnen, diesem Pfad für den Wechsel zu IMDSv2 zu folgen:

Schritt 1: Zu Beginn

Aktualisieren Sie die AWS-SDKs, die AWS CLI und Ihre Software, die Rollen-Anmeldeinformationen auf Ihren Instances verwendet, auf IMDSv2-kompatible Versionen. Informationen zum Upgrade der AWS CLI finden Sie unter Upgrade auf die neueste Version der AWS CLI im AWS Command Line Interface-Benutzerhandbuch.

Ändern Sie dann Ihre Software, die direkt auf Instance-Metadaten zugreift (mit anderen Worten, die kein AWS-SDK verwendet).

Schritt 2: Während des Wechsels

Verfolgen Sie den Wechselfortschritt mithilfe der Instance-Metrik `MetadataNoToken`. Diese Metrik zeigt die Anzahl der Aufrufe des Instance-Metadatenservices an, die IMDSv1 für Ihre Instances verwenden. Weitere Informationen finden Sie unter Anzeigen von Instance-Metriken.

Schritt 3: Wenn alles auf allen Instances bereit ist

Alles ist auf allen Instances fertig, wenn die Instance-Metrik `MetadataNoToken` keine IMDSv1-Nutzung verzeichnet. Auf dieser Stufe können Sie IMDSv2 auffordern, den Befehl update-instance-metadata-options zu verwenden. Sie können diese Änderungen an laufenden Instances vornehmen. Sie müssen Ihre Instances nicht neu starten.

Das Aktualisieren von Instance-Metadatenoptionen für vorhandene Instances ist nur über die Lightsail-API oder die AWS CLI verfügbar. Es ist derzeit nicht in der Lightsail-Konsole möglich. Weitere Informationen finden Sie unter Instance-Metadatenoptionen aktualisieren.

Zusätzliche IMDS-Dokumentation

Die folgende IMDS-Dokumentation ist im Benutzerhandbuch der Amazon Elastic Compute Cloud für Linux-Instances und im Benutzerhandbuch der Amazon Elastic Compute Cloud für Windows-Instances verfügbar:

> **Note**
>
> In Amazon EC2 werden Instance-Vorlagen als Amazon Machine Images (AMI) bezeichnet.

- Für Linux-Instances:
  - Konfigurieren der Instance-Metadaten-Optionen
  - Abrufen von Instance-Metadaten
  - Arbeiten mit Instance-Benutzerdaten
  - Abrufen von dynamischen Daten
  - Instance-Metadatenkategorien
  - Beispiel: AMI-Startindexwert
  - Instance-Identitätsdokumente
- Für Windows-Instances:
  - Konfigurieren der Instance-Metadaten-Optionen
  - Abrufen von Instance-Metadaten
  - Arbeiten mit Instance-Benutzerdaten
  - Abrufen von dynamischen Daten
  - Instance-Metadatenkategorien
  - Beispiel: AMI-Startindexwert
  - Instance-Identitätsdokumente

Blockspeicher-Datenträger in Amazon Lightsail

Systemdatenträger bieten die einheitliche Leistung und niedrige Latenz, die Sie zum Bewältigen Ihrer Workloads benötigen. Mit Lightsail-Datenträgern können Sie die genutzten Kapazitäten innerhalb von wenigen Minuten auf- und abskalieren und zahlen nur das, was Sie bereitstellen.

Sie können einen Systemdatenträger von bis zu 80 GB auf Ihrer Linux-/Unix- oder Windows Server-basierten Instance auswählen. Weitere Informationen finden Sie unter Erste Schritte mit Linux-/Unix-basierten Instances in Lightsail oder Erste Schritte mit Windows Server-basierten Instances.

Sie können Ihrem virtuellen privaten Server weiteren Speicherplatz hinzufügen, indem Sie zusätzliche Blockspeicher-Datenträger erstellen. Weitere Informationen finden Sie unter Blockspeicherfestplatten erstellen und an Ihre Linux-basierte Instance anhängen oder Blockspeicherfestplatten erstellen und an Ihre Windows Server-Instance anhängen.

Blockspeicher-Datenträger

Blockspeicher stellen eine Speicherarchitektur dar, die Daten als "Blöcke" verwaltet. Jeder Speicherblock (in Lightsail als "Datenträger" bezeichnet) funktioniert wie eine einzelne Festplatte, die Sie Ihrem Server anfügen können. Im Allgemeinen können Sie zusätzlichen Blockspeicher für Anwendungen oder Software verwenden, die spezielle Daten von ihrem Kernservice trennen und Anwendungsdaten schützen müssen, sollte es zu einem Ausfall kommen oder andere Probleme mit Ihrer Instance oder dem Boot-Speicherdatenträger auftreten.

Lightsail bietet SSD-Laufwerke (Solid-State Drives) für den Blockspeicher. Diese Art von Blockspeicher zeichnet sich durch ein gutes Preis-Leistungs-Verhältnis aus. Er wurde zur Unterstützung der meisten Workloads konzipiert, die auf Lightsail ausgeführt werden. Zusätzliche Lightsail-Blockspeicherdatenträger bieten Anwendungen und Software, die häufig auf gespeicherte Daten zugreifen müssen, konsistente Leistung und geringe Latenz.

> **Note**
>
> Für Kunden mit Anwendungen, die eine kontinuierliche IOPS-Leistung oder hohe Durchsatzraten pro Datenträger benötigen bzw. große Datenbanken wie MongoDB, Cassandra usw. ausführen, empfehlen wir die Verwendung von Amazon EC2 mit GP2 oder eines Bereitgestellte-IOPS-SSD-Speichers statt Lightsail.

Weitere Informationen zu Amazon-EBS-Volumes finden Sie im Benutzerhandbuch für Amazon EC2.

Datenträgerkontingente

- 20.000 GB pro Region
- Maximal 16 TB pro Datenträger oder mindestens 8 GB pro Datenträger
- Jede Instance kann bis zu 15 verbundene Datenträger und 1 Boot-Volume-Datenträger haben.

Erstellen von zusätzlichen Blockspeicherdatenträgern und Anfügen an Ihre Linux-basierte Lightsail-Instance

Sie können zusätzliche Blockspeicherdatenträger für Linux-basierte Lightsail-Instances erstellen und diesen anfügen. Nach dem Erstellen der Datenträger müssen Sie eine Verbindung mit der Linux-/Unix-basierten Lightsail-Instance herstellen und den Datenträger formatieren und mounten.

In diesem Thema wird das Erstellen und Anfügen eines neuen Datenträgers mithilfe von Lightsail behandelt. Außerdem wird beschrieben, wie Sie eine Verbindung mit der Linux-/Unix-basierten Instance über SSH herstellen, um den angefügten Datenträger zu formatieren und zu mounten.

Wenn Sie über eine Windows-Server-basierte Instance verfügen, finden Sie stattdessen weitere Informationen im Thema Erstellen von Blockspeicherdatenträgern und Anfügen an Windows-Server-basierte Instances.

Schritt 1: Erstellen Sie einen neuen Datenträger und fügen ihn an die Instance an

1. Wählen Sie auf der Lightsail-Startseite Storage (Speicher) aus.
2. Klicken Sie auf Datenträger erstellen.
3. Wählen Sie die AWS-Region und Availability Zone aus, in der sich Ihre Lightsail-Instance befindet.
4. Wählen Sie eine Größe.
5. Geben Sie einen Namen für Ihren Datenträger ein.

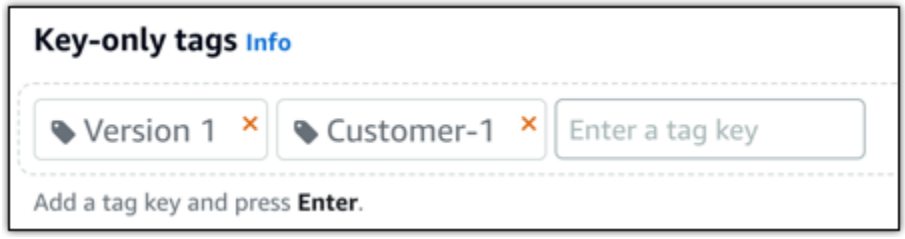
   Ressourcennamen:

   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.

- Muss zwischen 2 und 255 Zeichen enthalten.
- Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
- Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

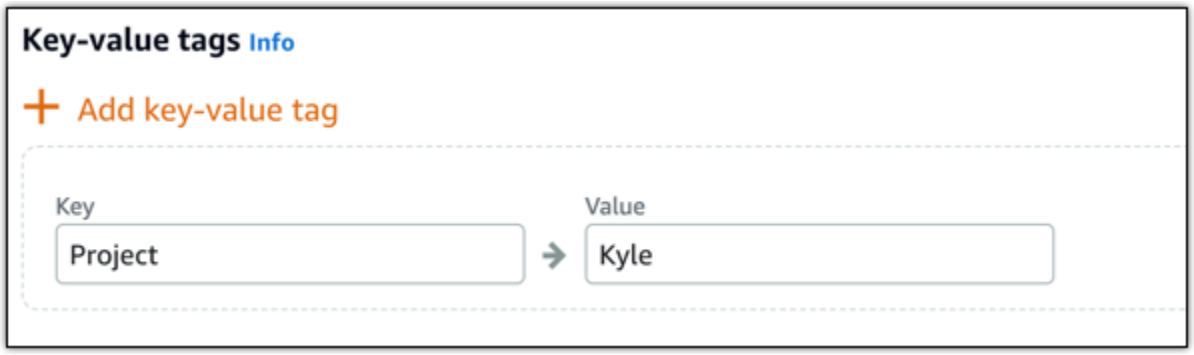
6. Wählen Sie eine der folgenden Optionen, um Ihrem Datenträger Tags hinzuzufügen:

- Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.



- Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

  Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.

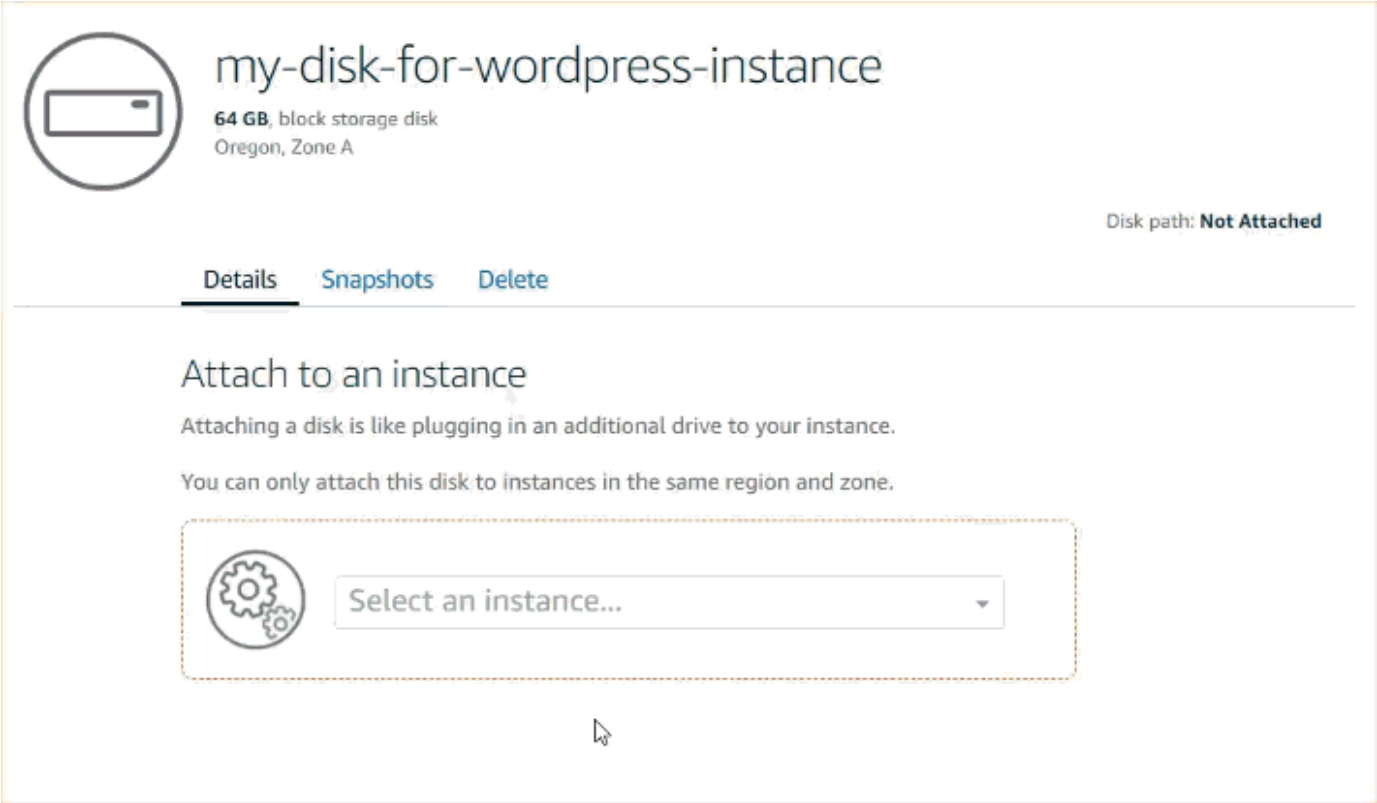


> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

7. Klicken Sie auf Datenträger erstellen.

   Nach einigen Sekunden wird der Datenträger erstellt und Sie befinden sich auf der Seite zur Verwaltung von neuen Datenträgern.

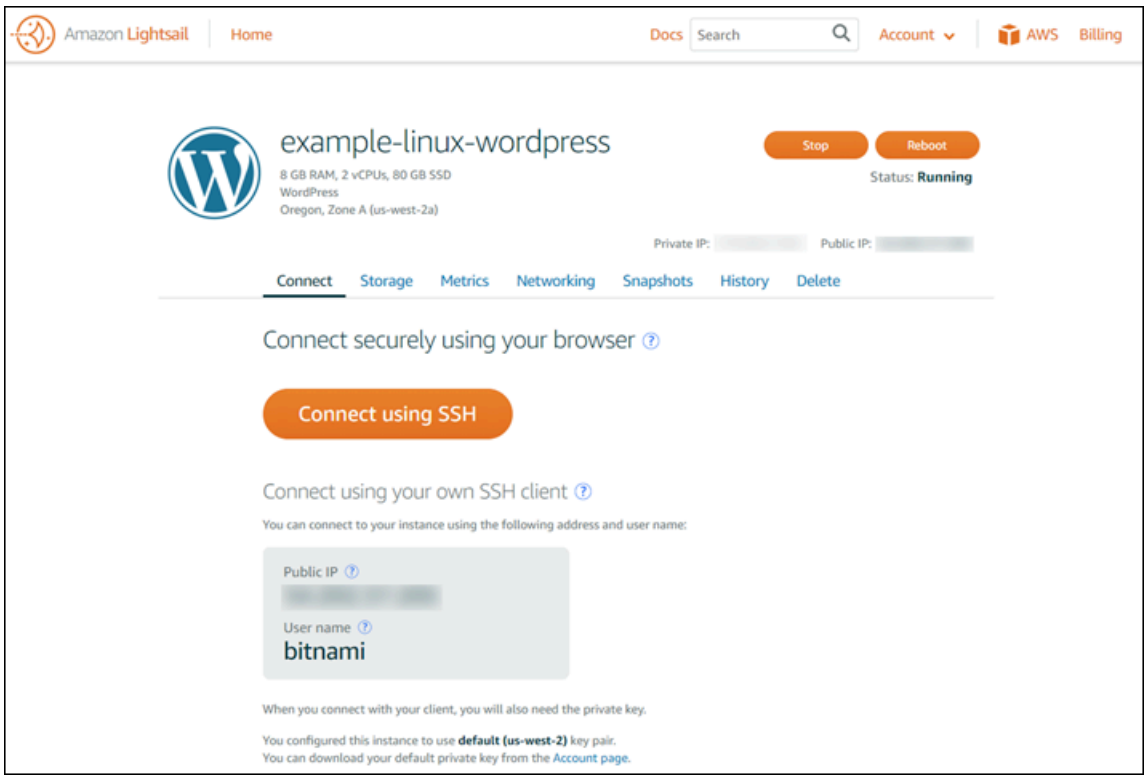
8. Wählen Sie Ihre Instance in der Liste aus und klicken Sie auf Attach (Anfügen), um Ihrer Instance den neuen Datenträger anzufügen.



Schritt 2: Stellen Sie eine Verbindung zu Ihrer Instance her und mounten Sie den Datenträger

1. Nachdem Sie den Datenträger erstellt und angefügt haben, wechseln Sie in Lightsail auf die Instance-Verwaltungsseite zurück.

   Standardmäßig wird die Registerkarte Connect (Verbinden) angezeigt.



2. Wählen Sie Connect using SSH (Mit SSH verbinden) aus, um eine Verbindung mit Ihrer Instance herzustellen.
3. Geben Sie Folgendes ein:

```
lsblk
```

Die Ausgabe sollte ungefähr wie die folgende aussehen.

```
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0  80G  0 disk
##xvda1 202:1    0  80G  0 part /
xvdf    202:80   0  64G  0 disk
```

In der Ausgabe für `lsblk` wird das Präfix `/dev/` aus den Datenträgerpfaden entfernt.

4. Bestimmen Sie, ob auf dem Datenträger ein Dateisystem erstellt werden muss. Neue Datenträger sind unformatierte Blockgeräte. Sie müssen ein Dateisystem auf ihnen erstellen, bevor Sie sie mounten und verwenden können. Datenträger, die anhand von Snapshots erstellt wurden, verfügen wahrscheinlich bereits über ein Dateisystem. Wenn Sie ein neues Dateisystem auf einem vorhandenen Dateisystem erstellen, werden Ihre Daten durch diesen Vorgang

überschrieben. Verwenden Sie den folgenden Befehl, um spezielle Informationen wie den Dateisystemtyp aufzulisten.

```
sudo file -s /dev/xvdf
```

Die Ausgabe für einen vollständig neuen Datenträger sollte folgendermaßen aussehen:

```
/dev/xvdf: data
```

Wenn Sie eine Ausgabe wie die folgende sehen, bedeutet dies, dass Ihr Datenträger bereits ein Dateisystem hat.

```
/dev/xvda1: Linux rev 1.0 ext4 filesystem data, UUID=1701d228-e1bd-4094-
a14c-12345EXAMPLE (needs journal recovery) (extents) (large files) (huge files)
```

5. Erstellen Sie mit dem folgenden Befehl ein ext4-Dateisystem auf dem Datenträger. Ersetzen Sie `/dev/xvdf`device_name *durch den Gerätenamen (wie*). Abhängig von den Anforderungen Ihrer Anwendung oder den Einschränkungen Ihres Betriebssystems können Sie ein anderes Dateisystem wie `ext3` oder XFS wählen.

   > **Important**
   >
   > Bei diesem Schritt wird vorausgesetzt, dass Sie einen leeren Datenträger mounten. Verwenden Sie den `mkfs`-Befehl nicht, wenn Sie einen Datenträger mounten, auf dem bereits Daten vorhanden sind (z. B. einen Datenträger, der von einem Snapshot wiederhergestellt wurde). Fahren Sie stattdessen mit Schritt 6 in diesem Verfahren fort und erstellen Sie einen Mounting-Punkt. Andernfalls formatieren Sie den Datenträger und löschen die vorhandenen Daten.

   ```
   sudo mkfs -t ext4 device_name
   ```

   Die Ausgabe sollte ungefähr wie die folgende aussehen.

   ```
   mke2fs 1.42.9 (4-Feb-2014)
   Filesystem label=
   OS type: Linux
   Block size=4096 (log=2)
   ```

```
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
4194304 inodes, 16777216 blocks
838860 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4294967296
512 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
4096000, 7962624, 11239424

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

6. Erstellen Sie mit dem folgenden Befehl das Verzeichnis für den Mounting-Punkt für den Datenträger. Der Mounting-Punkt ist die Position des Datenträgers in der Dateisystemstruktur. Hier werden außerdem nach dem Mounten des Datenträgers Dateien gelesen und geschrieben. Ersetzen Sie *mount_point* durch einen Speicherort wie z. B. `/data`.

   ```
   sudo mkdir mount_point
   ```

7. Geben Sie den folgenden Befehl ein, um zu überprüfen, ob der Datenträger jetzt über ein Dateisystem verfügt.

   ```
   sudo file -s /dev/xvdf
   ```

   Anstelle von `/dev/xvdf: data` sehen Sie in etwa die folgende Ausgabe.

   ```
   /dev/xvdf: Linux rev 1.0 ext4 filesystem data, UUID=0ee83fdf-e370-442e-
   ae38-12345EXAMPLE (extents) (large files) (huge files)
   ```

8. Mounten Sie zum Schluss den Datenträger, indem Sie den folgenden Befehl eingeben.

   ```
   sudo mount device_name mount_point
   ```

   Überprüfen Sie die Dateiberechtigungen der neuen Datenträgerbereitstellung, um sicherzustellen, dass Ihre Benutzer und die Anwendungen auf dem Datenträger schreiben

können. Weitere Informationen zu den Dateiberechtigungen finden Sie unter Verfügbarmachen eines Amazon-EBS-Volumes für die Verwendung im Amazon-EC2-Benutzerhandbuch.

Schritt 3: Mounten Sie den Datenträger bei jedem Neustart der Instance

Vermutlich möchten Sie diesen Datenträger bei jedem Neustart der Lightsail-Instance mounten. Wenn Sie dies nicht planen, ist dieser Schritt optional.

1. Sie können diesen Datenträger bei jedem Neustart des Systems mounten, indem Sie in der Datei `/etc/fstab` einen Eintrag für das Gerät hinzufügen.

   Erstellen Sie eine Sicherung der Datei `/etc/fstab` für den Fall, dass Sie diese Datei beim Bearbeiten versehentlich beschädigen oder löschen.

   ```
   sudo cp /etc/fstab /etc/fstab.orig
   ```

2. Öffnen Sie die Datei `/etc/fstab` mit einem Texteditor Ihrer Wahl, z. B. vim.

   Sie müssen vor dem Öffnen der Datei `sudo` eingeben, damit Sie die Änderungen speichern können.

3. Fügen Sie am Ende der Datei eine neue Zeile für den Datenträger in folgendem Format hinzu.

   ```
   device_name  mount_point  file_system_type  fs_mntops  fs_freq  fs_passno
   ```

   Die neue Zeile kann zum Beispiel folgendermaßen aussehen.

   ```
   /dev/xvdf /data ext4 defaults,nofail 0 2
   ```

4. Speichern Sie die Datei und beenden Sie den Text-Editor.

Erstellen eines Lightsail-Blockspeicher-Datenträgers zum Verbinden mit Ihrer Windows-Server-Instance

Wenn Sie zusätzlichen Speicherplatz benötigen, können Sie in Amazon Lightsail Blockspeicher-Datenträger erstellen und an Ihre Windows Server-Instance anfügen. Weitere Informationen über Blockspeicher-Datenträger finden Sie unter Blockspeicher-Datenträger.

In dieser Anleitung erfahren Sie, wie Sie einen neuen Blockspeicher-Datenträger erstellen und über die Lightsail-Konsole an Ihre Windows Server-Instance anfügen. Außerdem wird beschrieben, wie Sie mithilfe von RDP eine Verbindung mit Ihrer Windows Server-basierten Instance herstellen, damit Sie die Festplatte online bringen und initialisieren können.

Dieses Verfahren ist unter Windows Server 2016 und Windows Server 2012 R2 identisch.

> **Note**
>
> Wenn Sie über eine Linux- oder Unix-basierte Instance verfügen, finden weitere Informationen unter Erstellen und Anfügen von Datenträgern zu Ihren Linux- oder Unix-basierten Instances.

Schritt 1: Erstellen Sie einen neuen Blockspeicher-Datenträger und fügen ihn an Ihre Instance an

Erstellen Sie mithilfe der Amazon Lightsail-Konsole einen neuen Blockspeicher-Datenträger und fügen ihn an Ihre Instance an.

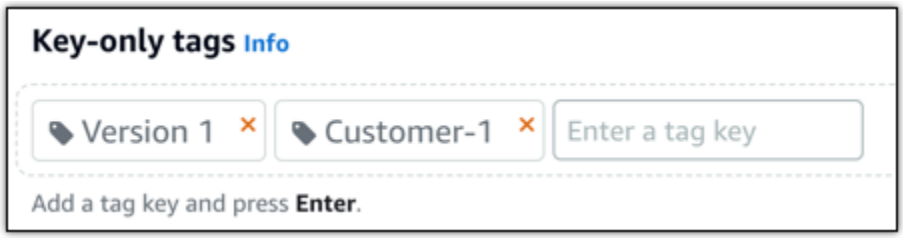
So erstellen Sie einen neuen Blockspeicher-Datenträger und fügen ihn an Ihre Instance an

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie die Registerkarte Storage (Speicher) und anschließend Create disk (Datenträger erstellen).
3. Wählen Sie die AWS-Region und Availability Zone aus, in der sich Ihre Lightsail-Instance befindet.
4. Wählen Sie ein Datenträgergröße.
5. Geben Sie einen Namen für Ihren Speicherdatenträger ein.

   Ressourcennamen:

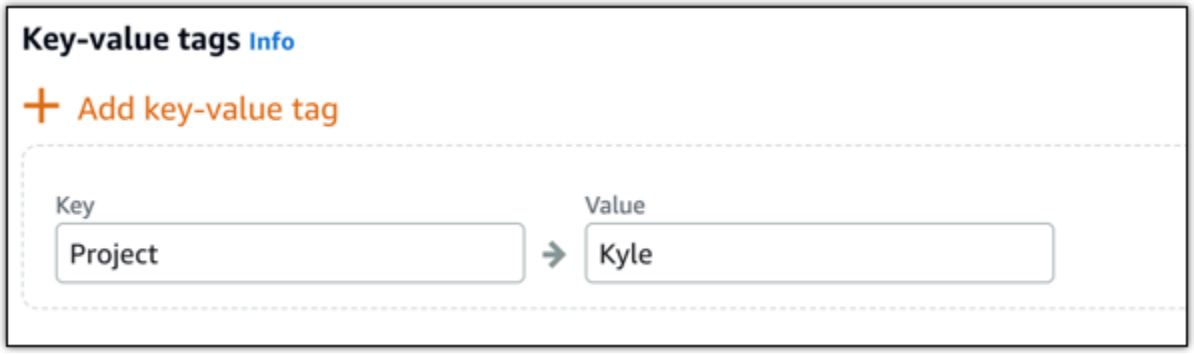
   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.
6. Wählen Sie eine der folgenden Optionen, um Ihrem Datenträger Tags hinzuzufügen:

- Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.



- Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

  Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.



> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

7. Klicken Sie auf Datenträger erstellen.

   Nach wenigen Sekunden ist der Datenträger erstellt und Sie können die entsprechenden Informationen über ihn auf der Seite für die Datenträgerverwaltung finden.

8. Wählen Sie Ihre Instance in der Liste aus und klicken Sie auf Attach (Anfügen), um Ihrer Instance den neuen Datenträger anzufügen.

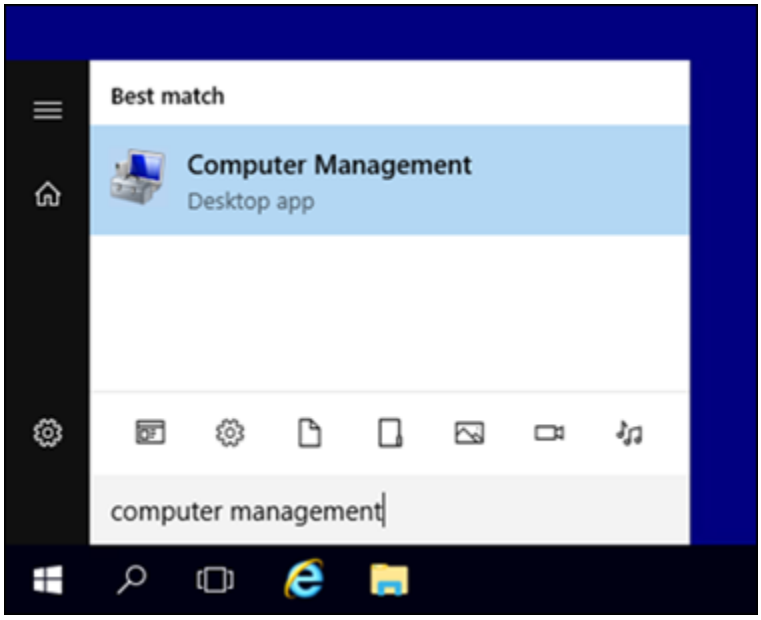
Fahren Sie mit dem Abschnitt Schritt 2: Verbinden mit der Instance und Onlinebringen des Blockspeicher-Datenträgers in diesem Handbuch fort, um den Blockspeicher-Datenträger online zu bringen.

Schritt 2: Verbinden mit der Instance und Onlinebringen des Blockspeicher-Datenträgers

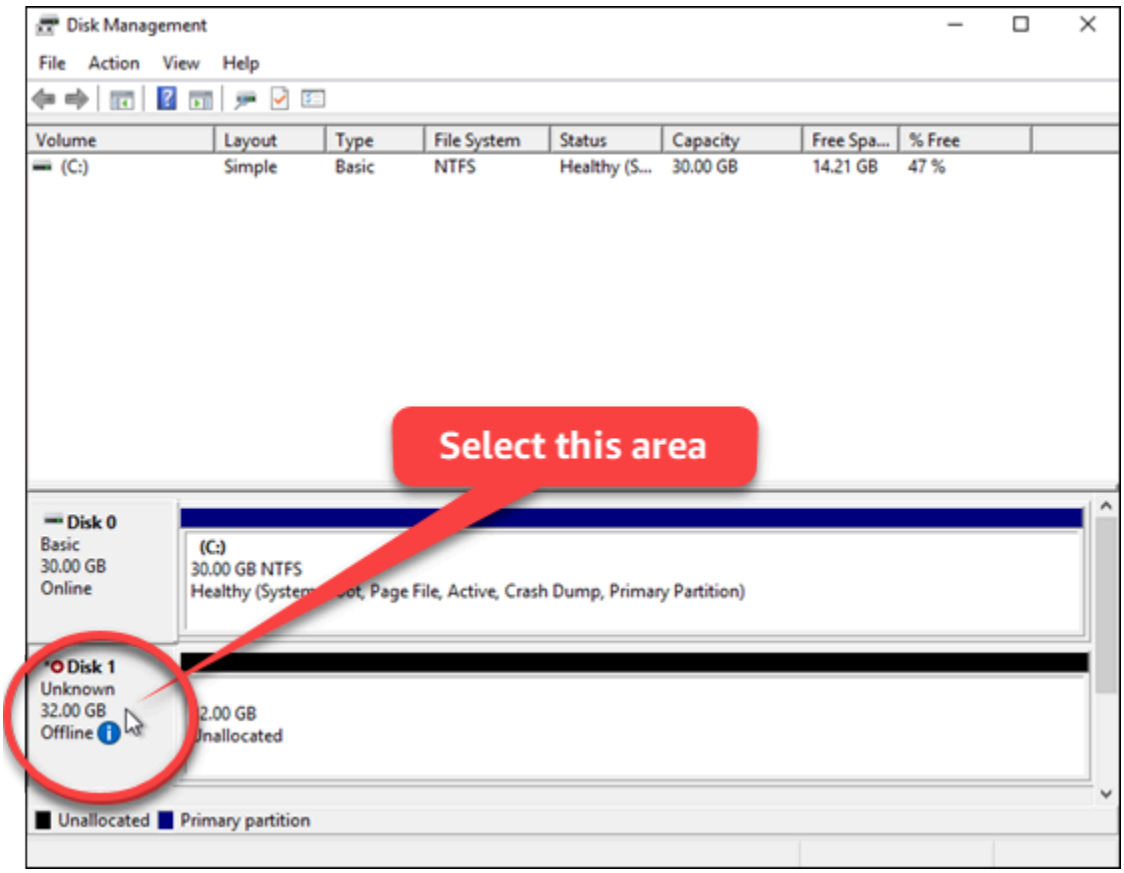
Verbinden Sie sich mit Ihrer Windows Server-Instance und verwenden Sie das Dienstprogramm Disk Management, um den kürzlich angefügten Blockspeicher-Datenträger online zu bringen.

So verbinden Sie sich mit Ihrer Instance und bringen den Blockspeicher-Datenträger online

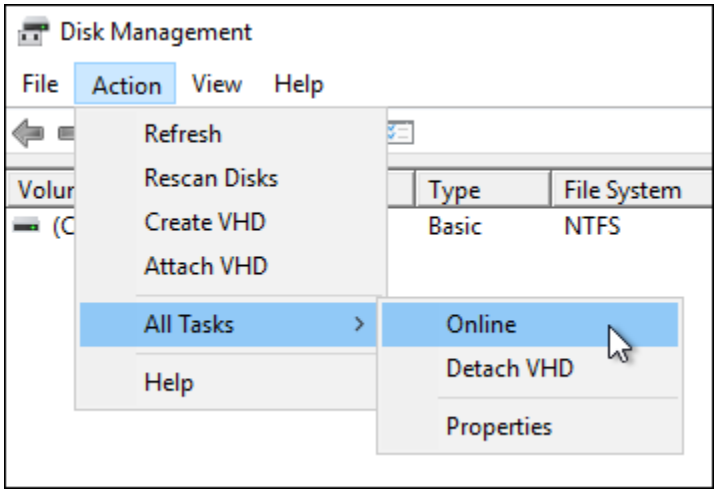
1. Navigieren Sie zur Startseite der Lightsail-Konsole.
2. Wählen Sie den Namen der Instance, an die Sie weiter oben in dieser Anleitung den zusätzlichen Datenträger angefügt haben.
3. Wählen Sie auf der Registerkarte Connect (Verbinden) die Option Connect using RDP (Verbinden über RDP).
4. Suchen Sie im Windows-Startmenü nach Computer Management (Computerverwaltung) und wählen Sie anschließend Computer Management (Computerverwaltung) aus.



5. Wählen Sie in der Computerverwaltung auf der linken Seite Disk Management (Festplattenverwaltung).
6. Wählen Sie im unteren Bereich des Dienstprogramms Disk Management das Laufwerk mit der Bezeichnung Unknown / Offline (Unbekannt/Offline). Dies ist der Blockspeicher-Datenträger, den Sie weiter oben in dieser Anleitung an Ihre Instance angefügt haben.



7. Während der Datenträger ausgewählt ist, zeigen Sie unter dem Menü Action (Aktion) auf All Tasks (Alle Aufgaben) und wählen anschließend Online aus.



Der Status des Blockspeicher-Datenträgers sollte auf Not Initialized (Nicht initialisiert) aktualisiert werden. Der Blockspeicher-Datenträger ist noch nicht online. Fahren Sie mit dem Abschnitt Schritt 3: Initialisieren des Blockspeicher-Datenträgers in diesem Handbuch fort, um den Blockspeicher-Datenträger zu initialisieren.

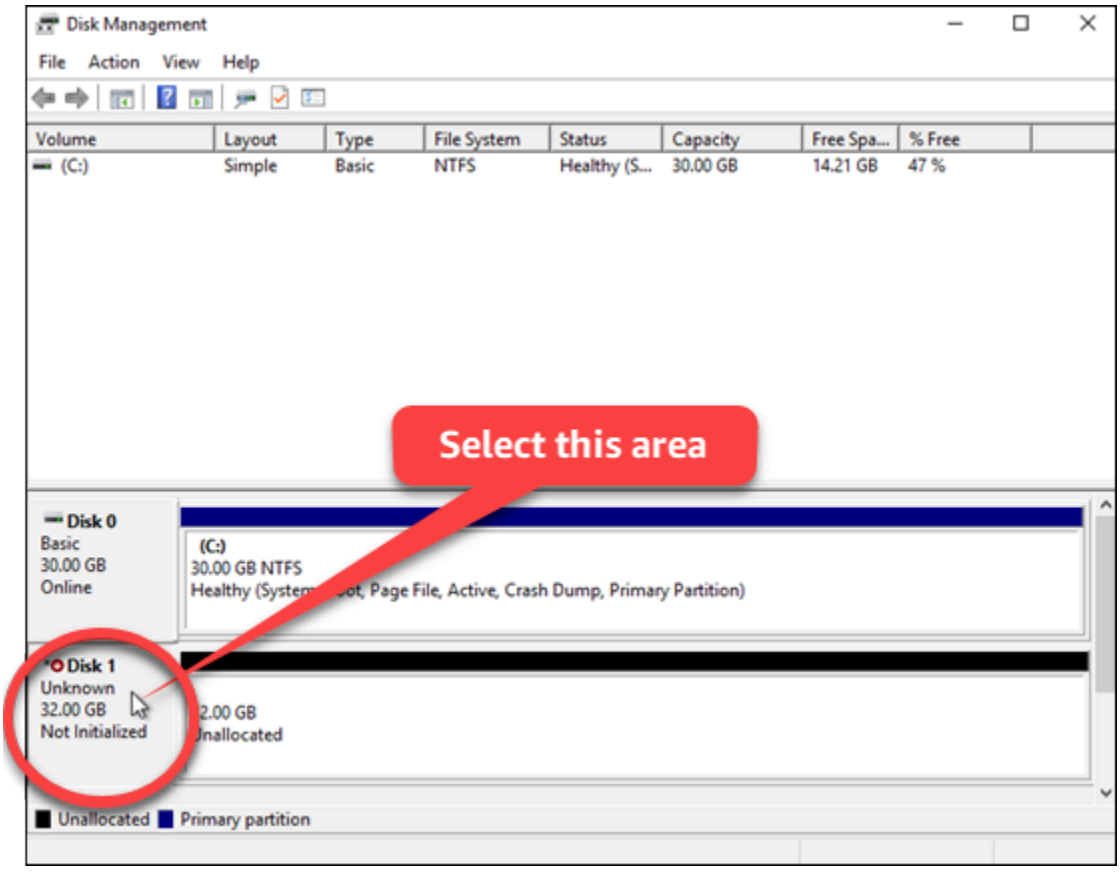
Schritt 3: Initialisieren des Blockspeicher-Datenträgers

Initialisieren Sie den Blockspeicher-Datenträger, damit Sie ihn formatieren können.

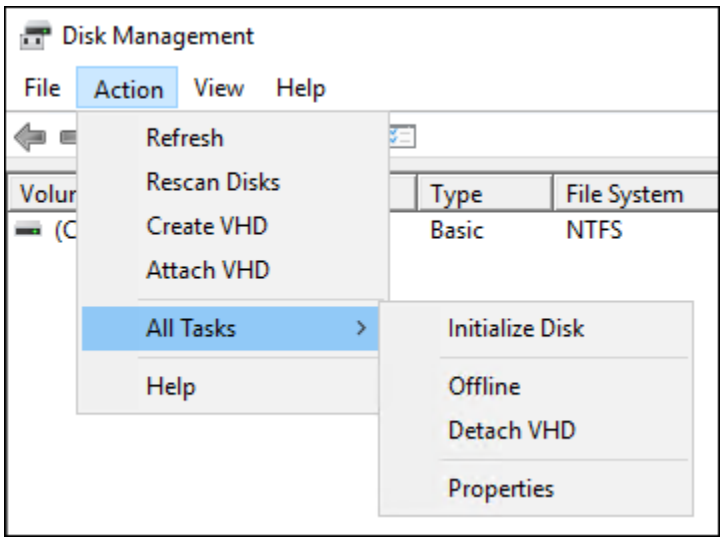
> **Important**
>
> Wenn Sie einen Datenträger mounten, auf dem bereits Daten vorhanden sind, wie etwa einen Datenträger, der aus einem Snapshot erstellt wurde, dürfen Sie den Datenträger nicht formatieren und dabei die vorhandenen Daten löschen.

So initialisieren Sie den Blockspeicher-Datenträger

1. Wählen Sie im unteren Bereich des Dienstprogramms Disk Management das Laufwerk mit der Bezeichnung Unknown / Not initialized (Unbekannt/Nicht initialisiert).



2. Während der Datenträger ausgewählt ist, zeigen Sie unter dem Menü Action (Aktion) auf All Tasks (Alle Aufgaben) und wählen anschließend Initialize Disk (Datenträger initialisieren) aus.



3. Wählen Sie den Partitionsstil für Ihren neuen Datenträger aus und klicken Sie anschließend auf OK.

> **Note**
>
> Weitere Informationen über Partitionsstile finden Sie im Artikel Über Partitionsstile - GPT und MBR von Microsoft.

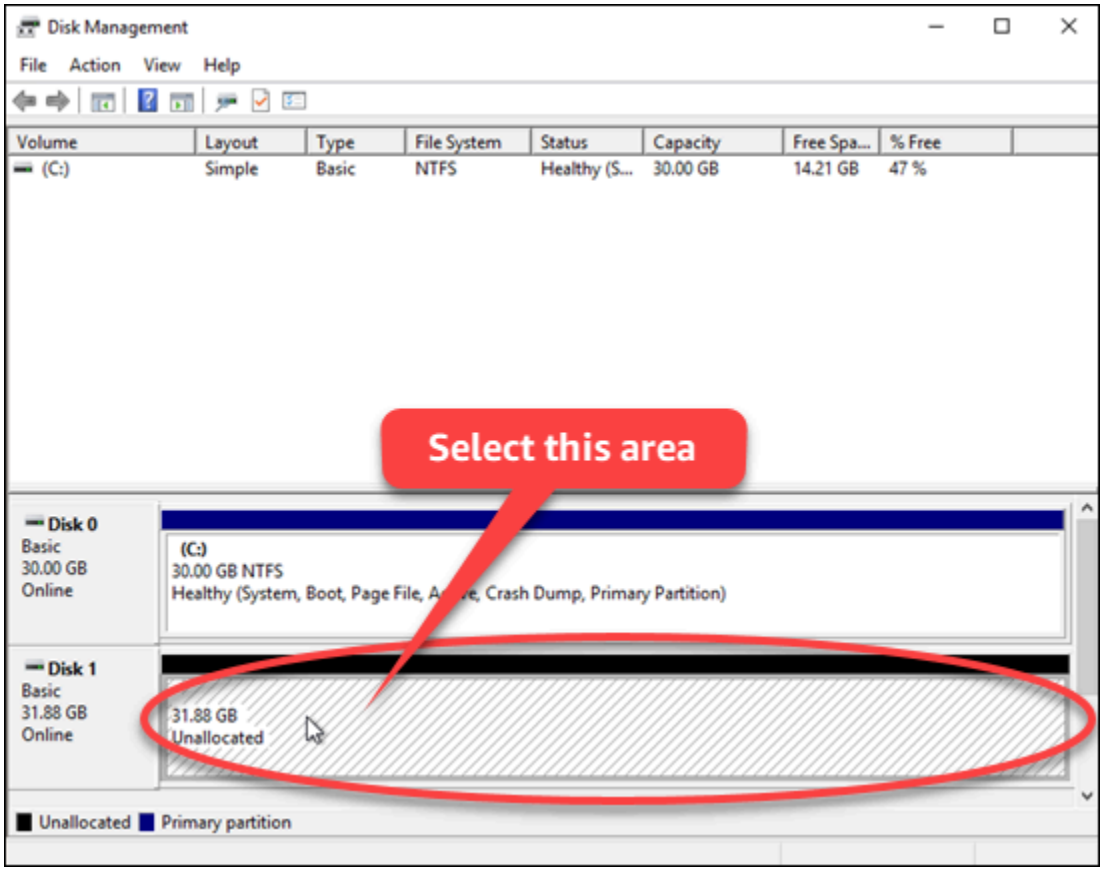
Der Status des Blockspeicher-Datenträgers sollte auf Online aktualisiert werden. Fahren Sie mit dem Abschnitt Schritt 4: Formatieren des Datenträgers mit einem Dateisystem in diesem Handbuch fort, um Ihren Blockspeicher-Datenträger mit einem Dateisystem zu formatieren.

Schritt 4: Formatieren des Datenträgers mit einem Dateisystem

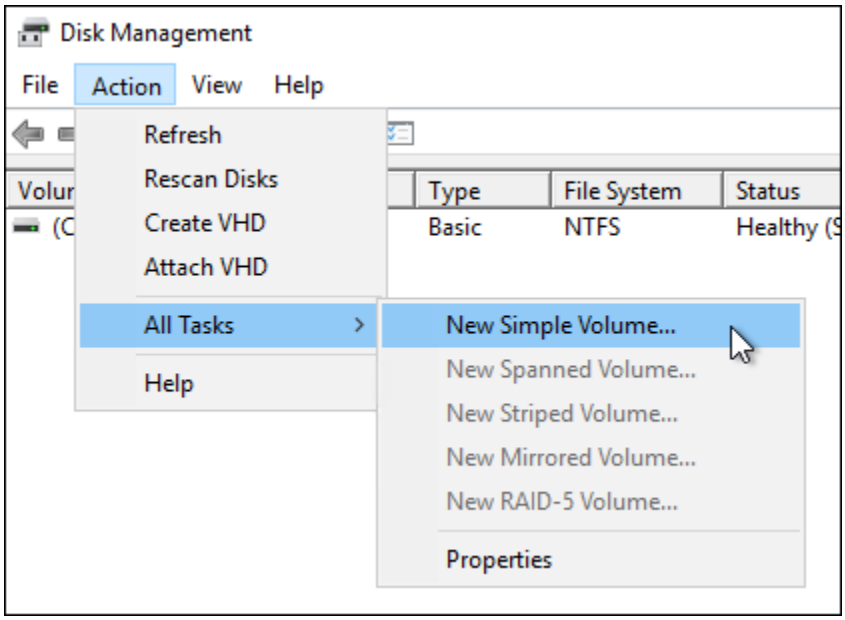
Verwenden Sie den New Simple Volume-Assistenten in Windows Server, um einen Laufwerkbuchstaben zuzuordnen und den Datenträger mit einem Dateisystem zu formatieren.

So formatieren Sie den Datenträger mit einem Dateisystem

1. Wählen Sie im unteren Bereich des Dienstprogramms Disk Management die Partition auf dem Blockspeicher-Datenträger mit der Bezeichnung Unallocated (Nicht zugeordnet) aus.



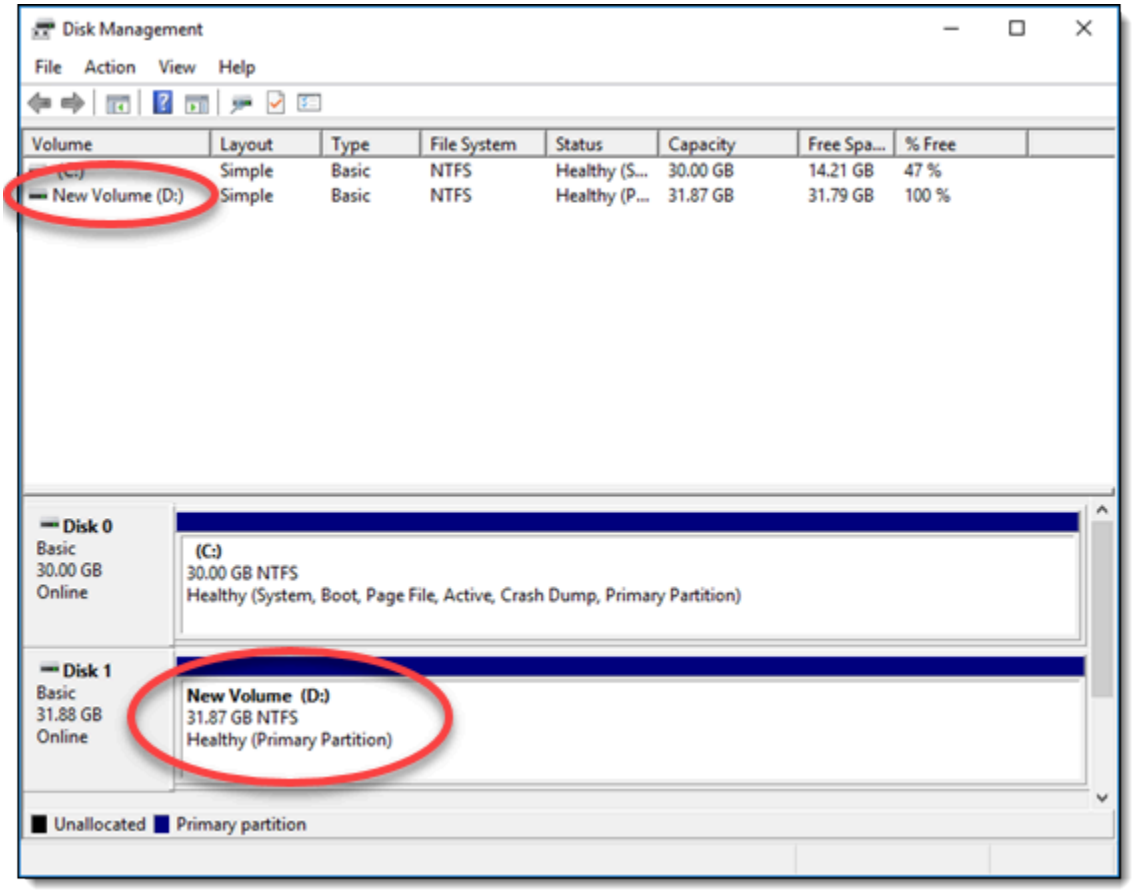
2. Wählen Sie, während die Partition ausgewählt ist, unter dem Menü Action (Aktion) die Option All Tasks (Alle Aufgaben), und wählen Sie anschließend New Simple Volume (Neues einfaches Volume) aus.



3. Befolgen Sie die Anweisungen im Assistenten New Simple Volume, um einen NTFS, FAT32 oder ReFS Dateisystemtyp auszuwählen und formatieren Sie den Datenträger.

> **Note**
>
> Weitere Informationen zu diesen Dateisystemen finden Sie in den Artikeln NTFS-Übersicht, Resilient File System (ReFS)-Übersicht und Beschreibung des FAT32 Dateisystems von Microsoft.

Wenn Sie fertig sind, sehen Sie einen Laufwerksbuchstaben und die folgende Meldung im Dienstprogramm Disk Management.



Trennen und Löschen eines Blockspeicherdatenträgers in Lightsail

Wenn Sie einen Blockspeicherdatenträger nicht mehr benötigen, können Sie ihn von der angehaltenen Lightsail-Instance trennen und anschließend löschen. In diesem Thema wird beschrieben, wie Sie Ihre Daten sichern und einen Datenträger sicher löschen.

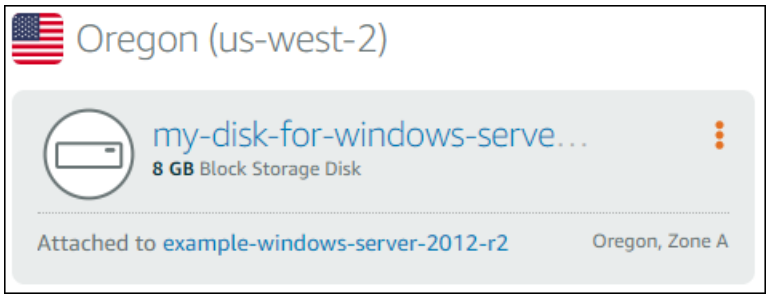
Voraussetzungen

- Halten Sie Ihre Instance an. Diesen Vorgang müssen Sie ausführen, bevor Sie den Datenträger trennen und anschließend löschen können. Erfahren Sie, wie Sie Ihre Instance anhalten.
- (Optional) Wir empfehlen, einen Snapshot Ihres Datenträgers zu erstellen. Auf diese Weise haben Sie eine Sicherung für den Fall, dass Sie es sich anders überlegen. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Datenbank

Trennen und Löschen Ihres Datenträgers

Sobald Sie Ihre Lightsail-Instance angehalten haben, können Sie Ihren Datenträger sicher trennen und löschen.

1. Wählen Sie auf der Startseite Storage (Speicher) aus.
2. Wählen Sie den Namen Ihres angefügten Datenträgers aus, um ihn zu verwalten.



3. Klicken Sie auf der Seite der Datenträgerverwaltung auf Detach (Trennen).

   Nach wenigen Sekunden wird der Datenträger getrennt und kann gelöscht oder neu angefügt werden.
4. Wählen Sie die Registerkarte Delete (Löschen) aus.
5. Wählen Sie Delete disk (Disk löschen) aus und bestätigen Sie den Vorgang mit Yes, delete (Ja, löschen).

> **Important**
>
> Dieser Vorgang ist dauerhaft und kann nicht rückgängig gemacht werden. Sie verlieren alle Daten auf dem Datenträger, wenn Sie ihn löschen.

Snapshots in Amazon Lightsail

Sie können point-in-time Snapshots von Instances, Datenbanken und Blockspeicherdatenträgern in Amazon Lightsail erstellen und diese als Baselines verwenden, um neue Ressourcen oder für Datensicherungen zu erstellen. Ein Snapshot enthält alle Daten, die erforderlich sind, um Ihre Ressource wiederherzustellen (ab dem Zeitpunkt, an dem der Snapshot erstellt wurde). Wenn Sie eine Ressource basierend auf einem Snapshot wiederherstellen, startet die neue Ressource als exakte Kopie der ursprünglichen Ressource, die zum Erstellen des Snapshots verwendet wurde. Ihnen wird eine Snapshot-Speichergebühr für Snapshots in Ihrem Lightsail-Konto in Rechnung gestellt, unabhängig davon, ob es sich um manuelle Snapshots, automatische Snapshots, kopierte Snapshots oder Systemdatenträger-Snapshots handelt. Wenn Sie eine Datenbeschädigung oder einen Festplattenausfall feststellen, können Sie einen Datenträger aus einem Snapshot erstellen, den Sie erstellt haben, und den alten Datenträger ersetzen. Sie können Snapshots auch verwenden, um neue Datenträger bereitzustellen und diese während eines neuen Instance-Starts anzufügen.

Inhalt

Manuelle Snapshots

Erstellen Sie jederzeit manuelle Snapshots von Instances, verwalteten Datenbanken und Blockspeicherdatenträgern. Manuelle Snapshots werden unbegrenzt gespeichert, bis Sie sie löschen.

Weitere Informationen zum Erstellen manueller Snapshots finden Sie in den folgenden Handbüchern:

- Erstellen eines Snapshots Ihrer Linux-/Unix-basierten Instance
- Erstellen eines Snapshots Ihrer Windows Server-Instance
- Einen Snapshot Ihrer Datenbank erstellen

- Erstellen eines Snapshots Ihres Blockspeicherdatenträgers

Automatische Snapshots

Wenn Sie wichtige Informationen auf Ihrer Lightsail-Instance oder Ihrem Blockspeicher-Datenträger hosten, sollten Sie diese häufig sichern, indem Sie manuelle Snapshots erstellen. Es ist jedoch nicht immer einfach, die Zeit für häufige Verwaltungsaufgaben zu finden. Wenn dies für Sie der Fall ist, verwenden Sie automatische Snapshots, damit Lightsail tägliche Backups Ihrer Instance oder Ihres Blockspeicher-Datenträgers in Ihrem Namen ohne manuelle Interaktion erstellt. Die letzten sieben automatischen Snapshots werden gespeichert, bevor der älteste durch den neuesten ersetzt wird.

Weitere Informationen zu automatischen Snapshots finden Sie in den folgenden Handbüchern:

- Aktivieren oder deaktivieren von automatischen Instance-Snapshots
- Ändern der automatischen Snapshot-Zeit für Instances oder Datenträger
- Löschen automatischer Snapshots

> **Important**
>
> Alle automatischen -Snapshots, die einer Ressource zugeordnet sind, werden gelöscht, wenn Sie die Quellressource löschen. Dieses Verhalten unterscheidet sich von manuellen Snapshots, die auch nach dem Löschen der Quellressource in Ihrem Lightsail-Konto aufbewahrt werden. Informationen zum Beibehalten der automatischen Snapshots beim Löschen der Quellressource finden Sie unter Aufbewahren automatischer Snapshots.

System-Datenträger-Snapshots

Wenn Ihre Instance nicht mehr reagiert und Sie auf die Dateien auf dem Systemdatenträger zugreifen müssen, können Sie das Instance-Stamm-Volume sichern, indem Sie einen Snapshot davon erstellen. Anschließend können Sie auf die Dateien im Systemdatenträger zugreifen, indem Sie einen neuen Blockspeicher-Datenträger aus dem Snapshot erstellen und einer anderen Instance anhängen. Weitere Informationen finden Sie unter Erstellen eines Snapshots eines Instance-Root-Volumes.

Erstellen neuer Ressourcen aus Snapshots

Verwenden Sie Snapshots, um neue Lightsail-Ressourcen mit demselben oder einem größeren Plan als die ursprüngliche Ressource zu erstellen. Wenn Sie eine Ressource basierend auf einem Snapshot erstellen, startet die neue Ressource als exakte Kopie der ursprünglichen Ressource, die zum Erstellen des Snapshots verwendet wurde. Snapshots können nicht verwendet werden, um neue Ressourcen mit einem kleineren Lightsail-Plan zu erstellen.

Weitere Informationen finden Sie in den folgenden Anleitungen:

- Erstellen einer Instance über einen Snapshot
- Eine Datenbank aus einem Snapshot erstellen
- Erstellen eines neuen Blockspeicherdatenträgers von einem Snapshot
- Erstellung einer größeren Instance, eines Blockspeicher-Datenträgers oder einer Datenbank aus einem Snapshot

Kopieren von Snapshots

Snapshots von Instance- und Blockspeicherdatenträgern können von einer Amazon Web Services (AWS)-Region in eine andere Region innerhalb desselben Lightsail-Kontos kopiert werden. Datenbank-Snapshots können nicht zwischen Regionen kopiert werden. Weitere Informationen finden Sie unter Kopieren von Snapshots von einer AWS-Region in eine andere .

Exportieren von Snapshots nach Amazon EC2

Lightsail ist der einfachste Weg, um mit zu beginnen AWS. Es gibt jedoch Einschränkungen bei Lightsail, die in Amazon EC2 oder anderen - AWS Services nicht vorhanden sind. Exportieren Sie Ihre Lightsail-Instance- und Blockspeicher-Datenträger-Snapshots nach Amazon EC2, um die Vorteile der breiteren Palette verfügbarer Instance-Typen zu nutzen und das gesamte Spektrum an Services in zu nutzen AWS. Weitere Informationen finden Sie unter Exportieren von Snapshots nach Amazon EC2.

> **Note**
>
> Snapshots von cPanel und WHM, Django und Ghost-Instances können derzeit nicht nach Amazon EC2 exportiert werden.

Snapshot löschen

Löschen Sie Lightsail-Snapshots, wenn Sie sie nicht mehr benötigen, um eine monatliche Snapshot-Speichergebühr zu vermeiden. Weitere Informationen finden Sie unter Löschen von Snapshots.

Erstellen eines Snapshots Ihres Lightsail-Blockspeicherdatenträgers

Sie können Datenträger-Snapshots in Lightsail als Backups Ihrer zusätzlichen Blockspeicher-Datenträger erstellen.

Sie können den Snapshot eines Datenträgers als Grundlage für neue Datenträger oder für die Datensicherung verwenden. Wenn Sie regelmäßig Snapshots von einem Datenträger erstellen, sind die Snapshots inkrementell. In einem neuen Snapshot werden nur die Blöcke auf den Geräten gespeichert, die sich seit dem letzten Snapshot geändert haben. Snapshots werden zwar inkrementell gespeichert, der Löschvorgang von Snapshots ist jedoch so konzipiert, dass Sie nur den aktuellen Snapshot benötigen, um den gesamten Datenträger wiederherzustellen.

Weitere Informationen finden Sie unter Snapshots.

1. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
2. Wählen Sie den Namen des Blockspeicherdatenträgers aus, für den Sie einen Snapshot erstellen möchten.
3. Wählen Sie die Registerkarte Snapshots aus.
4. Wählen Sie im Abschnitt Manual snapshots (Manuelle Snapshots) der Seite Create snapshot (Snapshot erstellen) und geben Sie dann einen Namen für Ihren Snapshot ein.

   Ressourcennamen:

   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.
5. Wählen Sie Erstellen aus.

   Sie können den soeben erstellten Snapshot mit dem Status Snapshotting... anzeigen.

Wenn der Snapshot fertig ist, können Sie einen anderen Datenträger aus dem Snapshot erstellen.

Erstellen eines neuen Lightsail-Blockspeicherdatenträgers von einem Snapshot

Sie können einen neuen Blockspeicher-Datenträger von einem Datenträger-Snapshot erstellen. Wenn Sie einen völlig neuen Datenträger erstellen, lesen Sie stattdessen das Thema zum Erstellen von zusätzlichen Blockspeicher-Datenträgern (Linux/Unix) oder zum Erstellen und Anfügen von Blockspeicher-Datenträgern an Ihre Windows-Server-Instance.

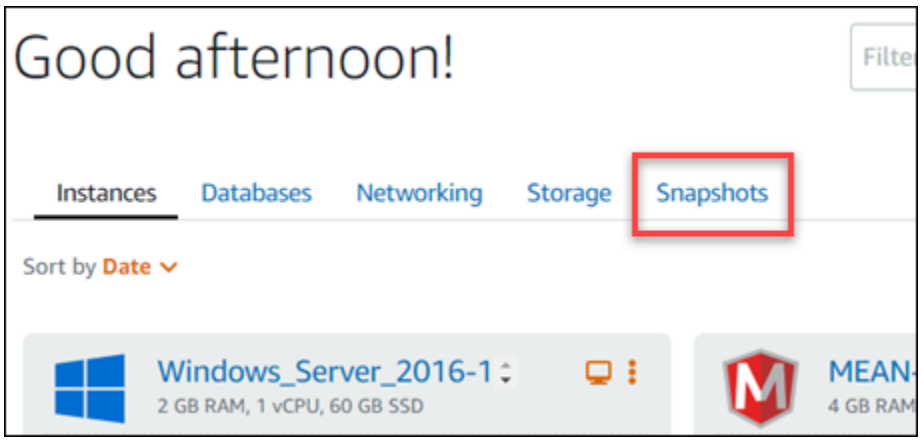
Sie können den Snapshot eines Blockspeicher-Datenträgers als Grundlage für neue Datenträger oder für die Datensicherung verwenden. Wenn Sie regelmäßig Snapshots von einem Datenträger erstellen, sind die Snapshots inkrementell. In einem neuen Snapshot werden nur die Blöcke auf dem Datenträger gespeichert, die sich seit dem letzten Snapshot geändert haben. Snapshots werden zwar inkrementell gespeichert, der Löschvorgang von Snapshots ist jedoch so konzipiert, dass Sie nur den aktuellen Snapshot benötigen, um den gesamten Datenträger wiederherzustellen. Informationen zum Erstellen eines Snapshots Ihres Blockspeicher-Datenträgers finden Sie unter Erstellen eines Snapshots Ihres Blockspeicher-Datenträgers.

Schritt 1: Suchen des Datenträger-Snapshots und Auswahl der Option zum Erstellen eines neuen Datenträgers

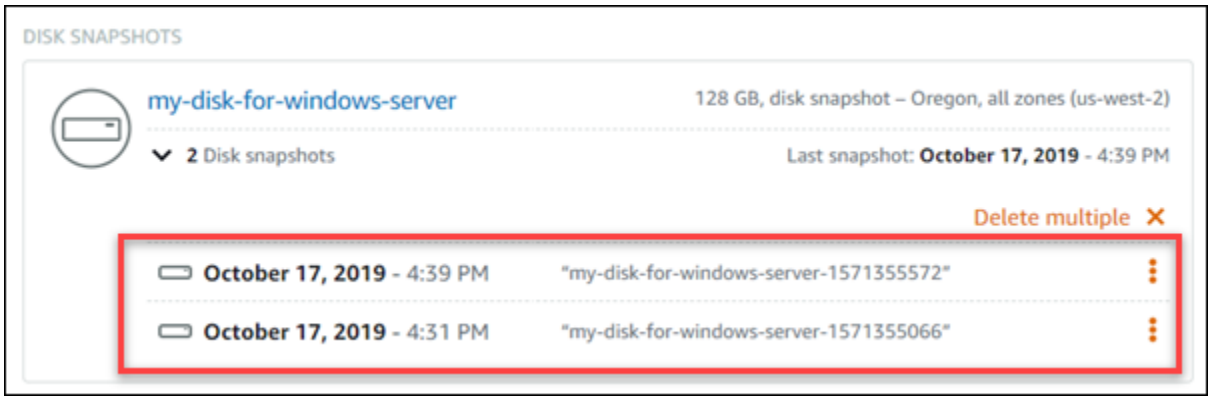
Sie können eine neue Instance von einem Datenträger-Snapshot an einen von zwei Orten in Lightsail erstellen: auf der Registerkarte Snapshots der Lightsail-Startseite oder auf der Registerkarte Snapshots der Seite zur Datenträgerverwaltung.

Auf der Lightsail-Startseite

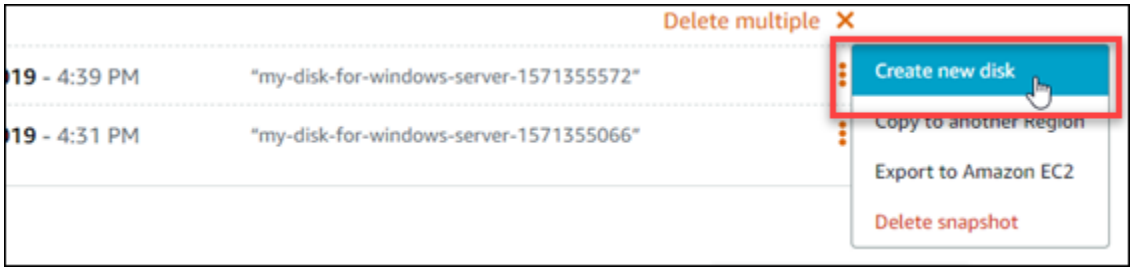
1. Wählen Sie auf der Lightsail-Startseite Snapshots aus.



2. Suchen Sie den Namen des Datenträgers und erweitern Sie dann den Knoten darunter, um alle verfügbaren Snapshots dieses Datenträgers anzuzeigen.

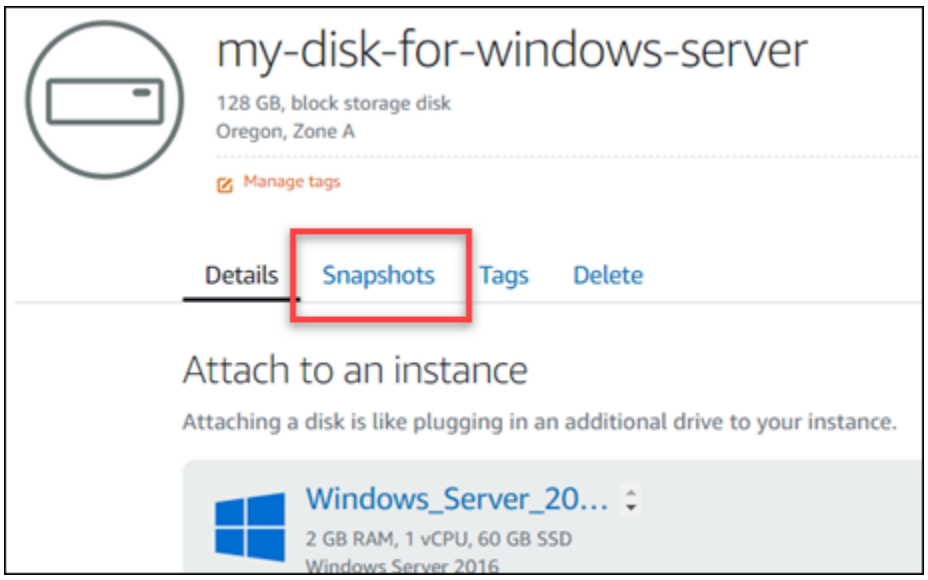


3. Klicken Sie das Aktionsmenüsymbol (:) neben dem Snapshot, auf dessen Grundlage Sie den neuen Datenträger erstellen möchten, und wählen Sie dann Create new disk (Neuen Datenträger erstellen) aus.

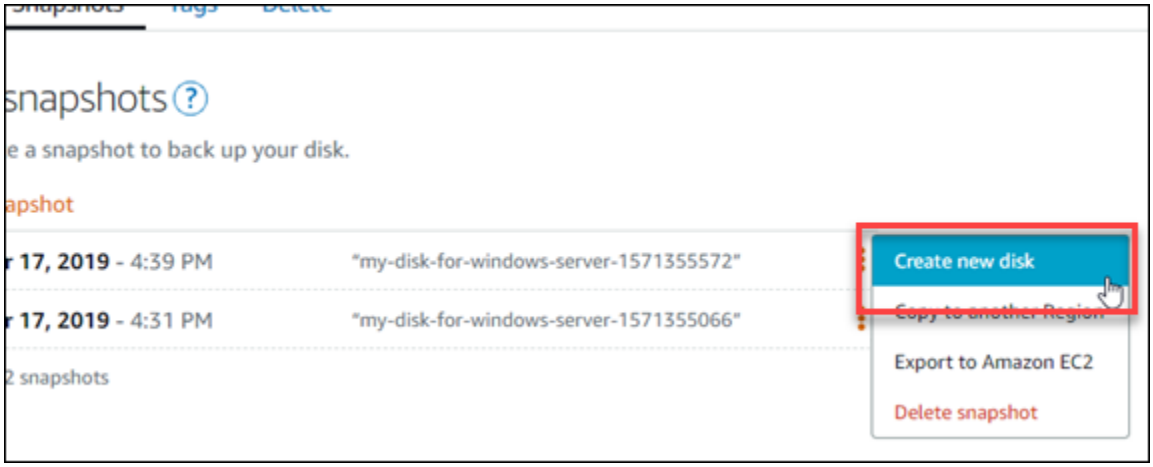


Auf der Seite für die Datenträgerverwaltung in Lightsail

1. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
2. Wählen Sie den Namen des Datenträgers aus, für den Sie Snapshots anzeigen möchten.
3. Wählen Sie die Registerkarte Snapshots aus.



4. Wählen Sie im Abschnitt Manual snapshots (Manuelle Snapshots) der Seite das Aktionsmenüsymbol (⋮) neben dem Snapshot aus, aus dem Sie einen neuen Datenträger erstellen möchten, und wählen Sie Create new disk (Neuen Datenträger erstellen) aus.



Schritt 2: Erstellen eines neuen Datenträgers von einem Datenträger-Snapshot

1. Wählen Sie eine Availability Zone für den neuen Datenträger aus oder akzeptieren Sie die Standardeinstellung (z. B. `us-east-2a`).

   Sie müssen den neuen Datenträger in derselben AWS-Region erstellen, in der sich der Quelldatenträger befindet.

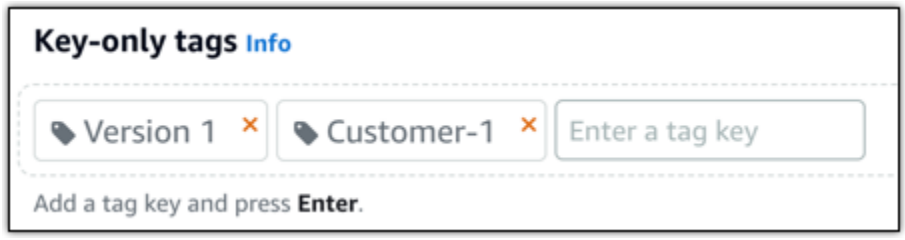
2. Legen Sie eine Größe für den neuen Datenträger fest, die größer oder gleich der Größe des Snapshots ist.
3. Geben Sie einen Namen für Ihren Datenträger ein.

Ressourcennamen:

- Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
- Muss zwischen 2 und 255 Zeichen enthalten.
- Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
- Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

4. Wählen Sie eine der folgenden Optionen, um Ihrem Datenträger Tags hinzuzufügen:

   - Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.

   - Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

     Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.

> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

5. Klicken Sie auf Create disk (Datenträger erstellen).

Erstellen eines Snapshots eines Lightsail-Instance-Root-Volumes

Sichern Sie ein Instance-Root-Volume in Amazon Lightsail, indem Sie einen Snapshot der Systemfestplatte erstellen. Anschließend greifen Sie auf die Dateien in der Sicherung durch Erstellung eines neuen Blockspeicher-Datenträgers aus dem Snapshot und das Anhängen einer anderen Instance zu. Wählen Sie diese Option, wenn Sie Folgendes tun müssen:

- Wiederherstellen von Daten aus dem Root-Volume einer beschädigten Instance.
- Erstellen einer Sicherung des Root-Volumes Ihrer Instance, wie für einen Blockspeicher-Datenträger.

Sie erstellen den Instance-Root-Volume-Snapshot mit der AWS Command Line Interface (AWS CLI). Nachdem Sie den Snapshot erstellt haben, verwenden Sie die Lightsail-Konsole zum Erstellen eines Blockspeicher-Datenträgers aus dem Snapshot. Anschließend fügen Sie diesen an eine ausgeführte Instance an, und greifen von dieser Instance darauf zu.

Inhalt

Schritt 1: Erfüllen der Voraussetzungen

Falls noch nicht erfolgt, installieren und konfigurieren Sie die AWS CLI. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

Schritt 2: Erstellen eines Instance-Root-Volume-Snapshots

Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster, und geben Sie dann den folgenden Befehl ein, um einen Instance-Root-Volume-Snapshot zu erstellen.

```
aws lightsail create-disk-snapshot --region AWSRegion --instance-name InstanceName --
disk-snapshot-name DiskSnapshotName
```

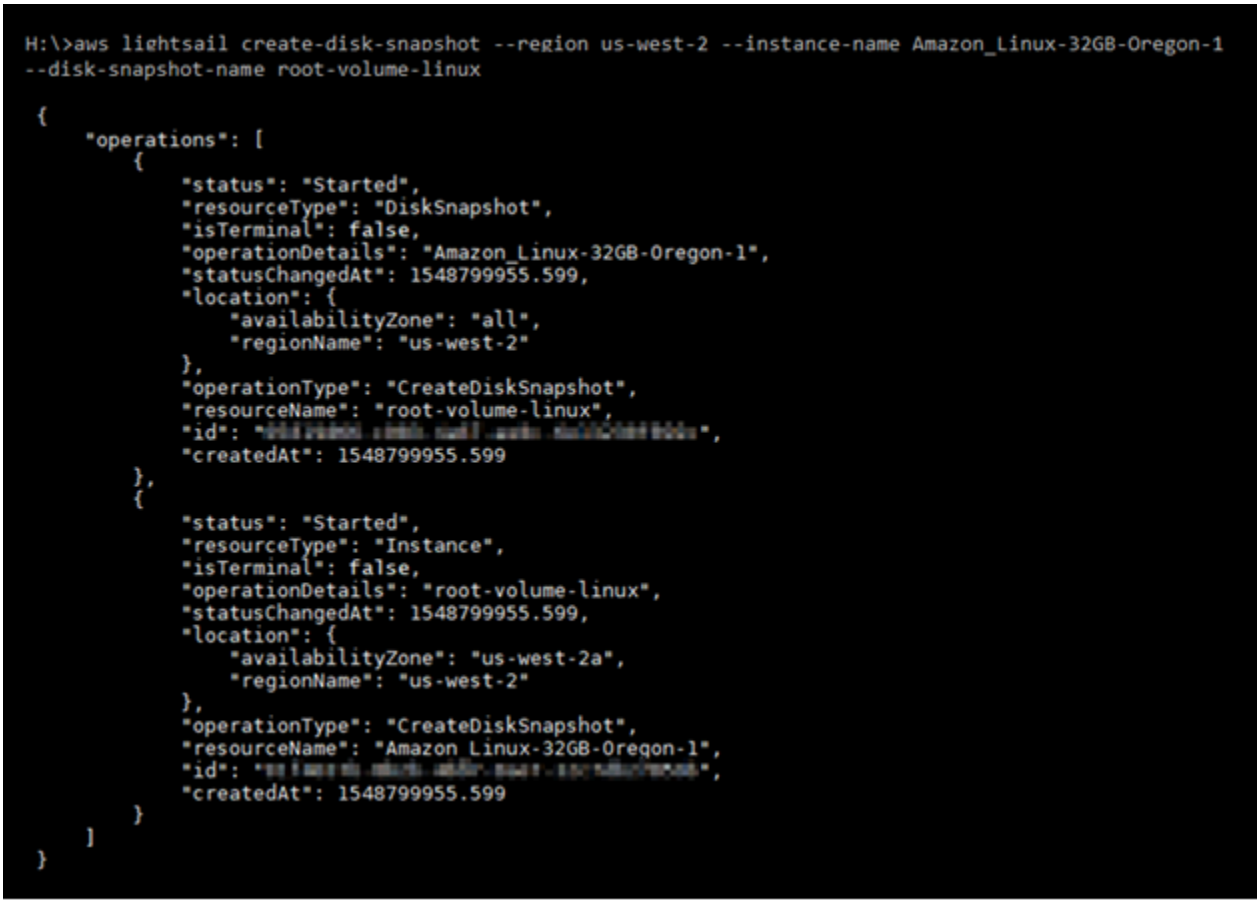
Ersetzen Sie im Befehl Folgendes:

- *AWSRegion* durch die AWS-Region der Instance.
- *InstanceName* durch den Namen der Instance, deren Root-Volume Sie sichern möchten.
- *DiskSnapshotName* durch den Namen des neuen Datenträger-Snapshots, der erstellt werden soll.

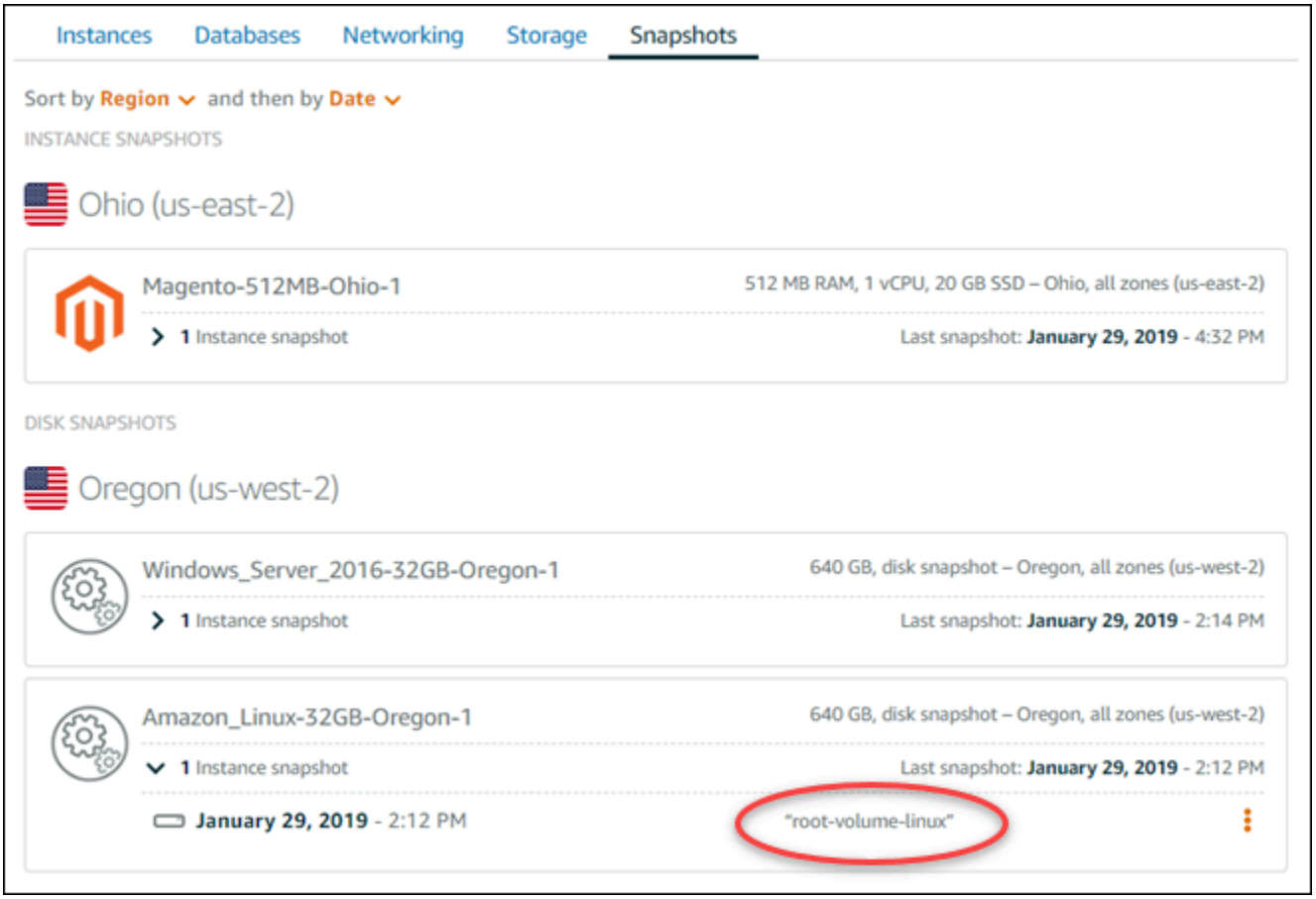
Beispiel:

```
aws lightsail create-disk-snapshot --region us-west-2 --instance-
name Amazon_Linux-32MB-Oregon-1 --disk-snapshot-name root-volume-linux
```

Ist der Befehl erfolgreich, sehen Sie ein Ergebnis, das etwa wie folgt aussieht:



Warten Sie einige Minuten, bis der Snapshot erstellt ist. Nachdem er erstellt wurde, können Sie ihn auf der Lightsail-Startseite anzeigen, indem Sie die Registerkarte Snapshots auswählen und einen Bildlauf zum Abschnitt „Disk Snapshots“ durchführen, wie im nachfolgenden Beispiel gezeigt.



Schritt 3: Erstellen eines Blockspeicher-Datenträgers aus einem Snapshot und Anhängen an eine Instance

Erstellen Sie einen neuen Blockspeicher-Datenträger aus dem Instance-Root-Volume-Snapshot und hängen Sie ihn an eine andere Instance an, wenn Sie auf deren Inhalte zugreifen müssen. Wählen Sie diese Option, wenn Sie Daten von einem Root-Volume einer beschädigten Instance wiederherstellen müssen.

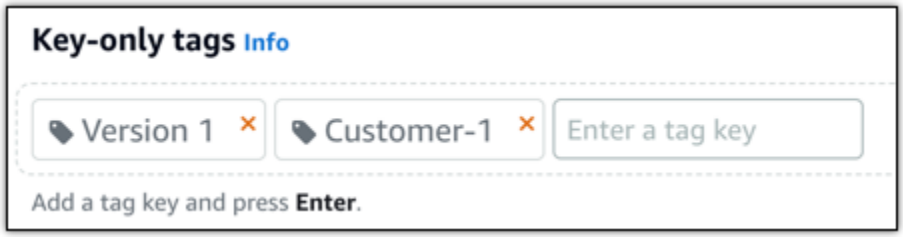
> **Note**
>
> Der neue Blockspeicher-Datenträger wird in derselben AWS-Region wie der Quell-Snapshot erstellt. Kopieren Sie zum Erstellen des Blockspeicher-Datenträgers in einer anderen Region den Snapshot in die gewünschte Region und erstellen Sie dann einen neuen Datenträger aus dem kopierten Datenträger. Weitere Informationen finden Sie unter Kopieren von Snapshots von einer AWS-Region in eine andere.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite Snapshots aus.
3. Wählen Sie das Aktionsmenüsymbol (⋮) neben dem Root-Volume-Datenträger-Snapshot, drn Sie verwenden möchten, und wählen Sie dann Create new disk (Neuen Datenträger erstellen).
4. Wählen Sie eine Availability Zone für den neuen Datenträger aus oder akzeptieren Sie die Standardeinstellung.
5. Legen Sie eine Größe für den neuen Datenträger fest, die größer oder gleich der Größe des Snapshots ist.
6. Geben Sie einen Namen für den Datenträger ein.

   Ressourcennamen:

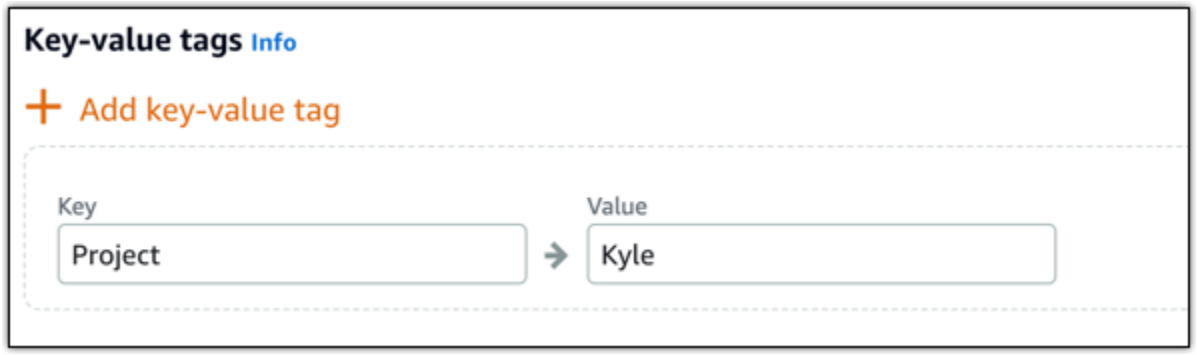
   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.
7. Wählen Sie eine der folgenden Optionen, um Ihrem Datenträger Tags hinzuzufügen:

   - Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.

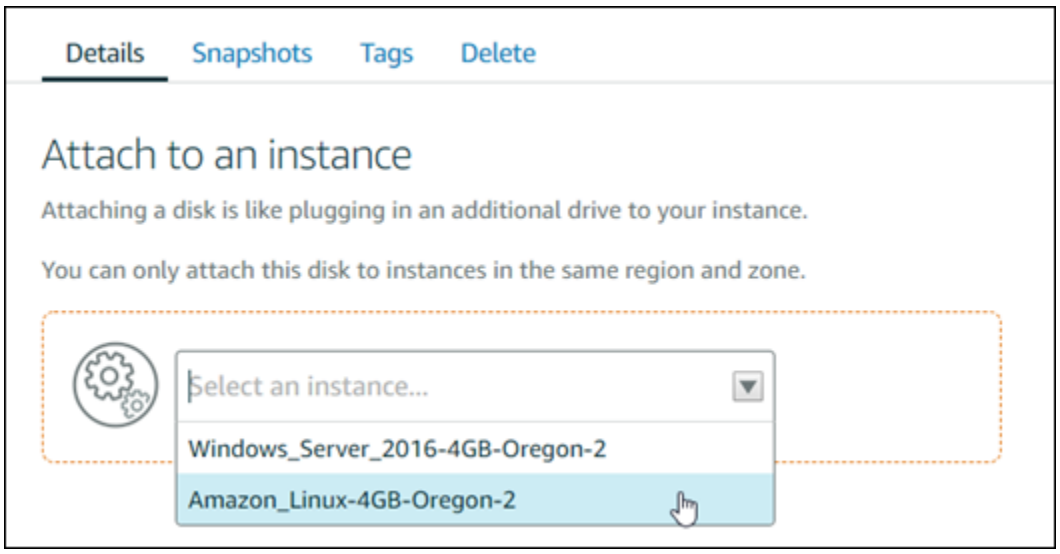
   - Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

     Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.



> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

8. Klicken Sie auf Create disk (Datenträger erstellen).
9. Nachdem der Datenträger erstellt wurde, wählen Sie die Instance, der Sie den Datenträger hinzufügen möchten, im Dropdownmenü Select an instance (Eine instance auswählen). Dies wird im folgenden Beispiel veranschaulicht.



10. Wählen Sie Attach (Anfügen) zum Anfügen des Datenträgers an die ausgewählte Instance.

    Der Datenträger ist jetzt an die Instance angehängt. Machen Sie ihn dann für das jeweilige Betriebssystem zugänglich, indem Sie ihn auf Linux mounten oder auf Windows online bringen. Weitere Informationen finden Sie im folgenden Abschnitt Zugriff auf den Blockspeicher von einer Instance aus in dieser Anleitung.

Schritt 4: Zugreifen auf einen Blockspeicher-Datenträger von einer Instance aus

Um auf einen Blockspeicher-Datenträger zuzugreifen, nachdem er einer Instance angehängt wurde, müssen Sie ihn auf Linux oder Unix mounten oder auf Windows online bringen.

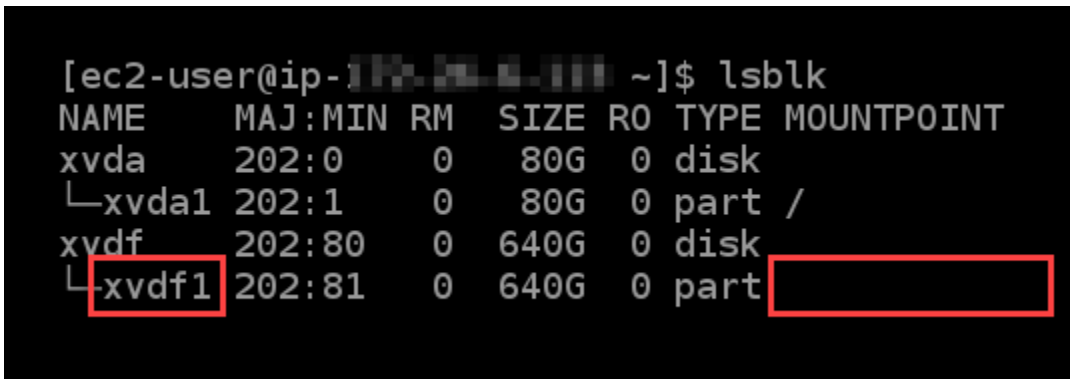
Mounten und Zugreifen auf einen Blockspeicher-Datenträger auf einer Linux- oder Unix-Instance

1. Wählen Sie auf der Lightsail Startseite das browserbasierte SSH-Client-Symbol für die Linux- oder Unix-Instance, an die Sie den Blockspeicher-Datenträger angefügt haben.

2. Nachdem der browserbasierte SSH-Client verbunden wurde, geben Sie den folgenden Befehl ein, um die an die Instance angehängten Blockspeicher-Datenträgergeräte anzuzeigen.

```
lsblk
```

   Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten: In diesem Beispiel ist `xvdf1` der Blockspeicher, der der Instance angefügt, aber noch nicht gemountet ist, da ein Mountingpunkt fehlt. Dazu ist bei dem Ergebnis `/dev/` aus dem Gerätenamen weggelassen, so dass der Name tatsächlich `/dev/xvdf1` ist.



3. Geben Sie den folgenden Befehl ein, um einen Mountingpunkt für den Blockspeicher-Datenträger zu erstellen.

```
sudo mkdir MountPoint
```

Ersetzen Sie im Befehl *MountPoint* durch den Namen des Verzeichnisses, in dem der Blockspeicher-Datenträger gemountet und zugänglich ist.

Beispiel:

```
sudo mkdir xvdf
```

4. Geben Sie den folgenden Befehl ein, um den Blockspeicher-Datenträger zu dem Mountingpunkt zu mounten, den Sie im vorhergehenden Schritt erstellt haben.

```
sudo mount /dev/DeviceName MountPoint
```

Ersetzen Sie im Befehl Folgendes:

- *DeviceName* durch den Namen des Blockspeicher-Datenträgergeräts.
- *MountPoint* durch das Mountingpunkt-Verzeichnis, das Sie im vorherigen Schritt erstellt haben.

Beispiel:

```
sudo mount /dev/xvdf1 xvdf
```

5. Geben Sie den folgenden Befehl aus, um die Blockspeicher-Datenträger, die der Instance angefügt sind, anzuzeigen:

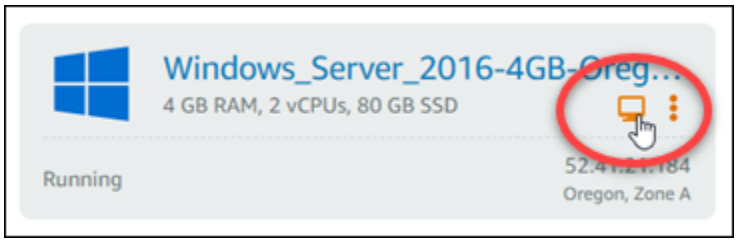
```
lsblk
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten: In diesem Beispiel ist das Gerät *xvdf1* jetzt gemountet und zugänglich im Verzeichnis */home/ec2-user/xvdf*. Sie können jetzt auf den Blockspeicher-Datenträger und seinen Inhalt zugreifen, indem Sie zum Mountingpunkt-Verzeichnis wechseln.

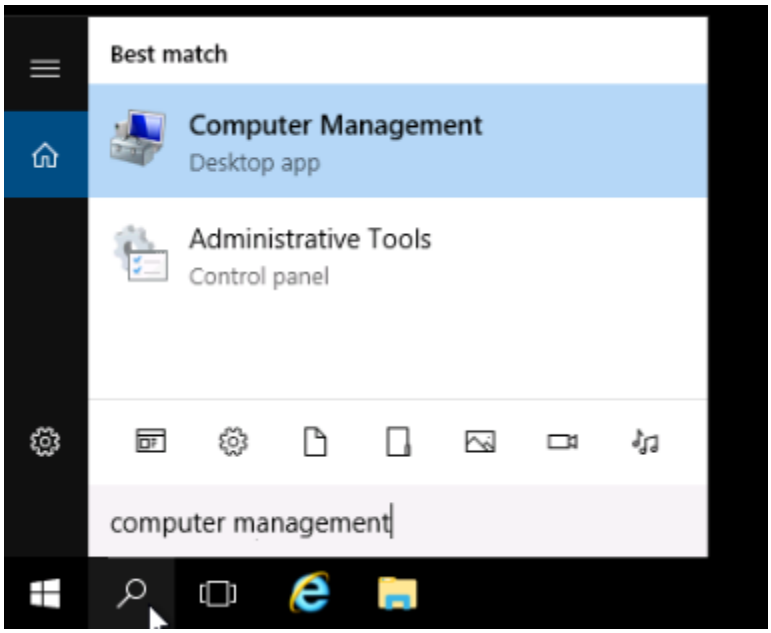
```
[ec2-user@ip-[redacted] ~]$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0   80G  0 disk
└─xvda1 202:1    0   80G  0 part /
xvdf    202:80   0  640G  0 disk
└─xvdf1 202:81   0  640G  0 part /home/ec2-user/xvdf
```

Bringen eines Blockspeicher-Datenträger online und Zugriff darauf auf einer Windows-Instance

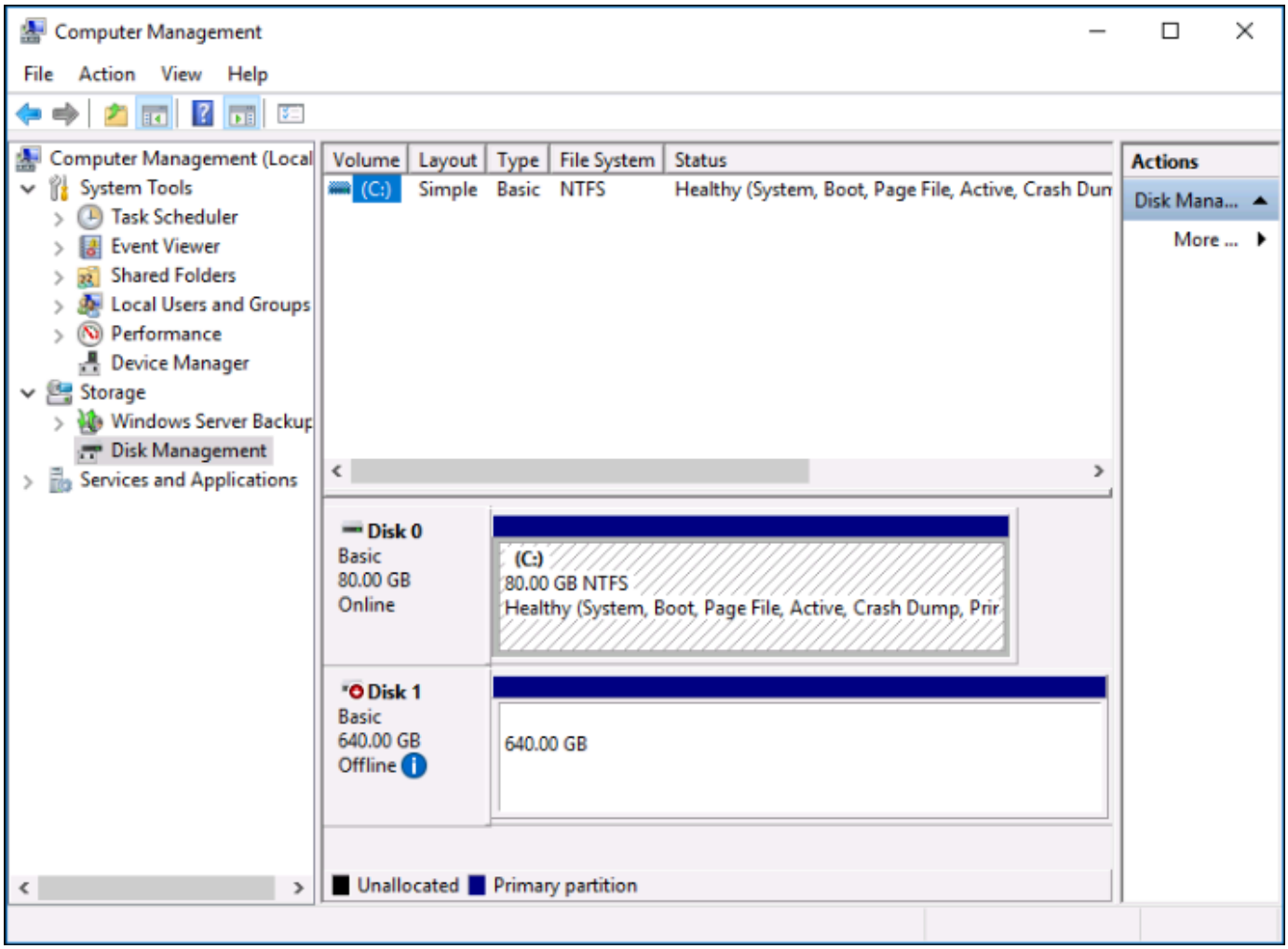
1. Wählen Sie auf der Lightsail-Startseite das browserbasierte RDP-Client-Symbol für die Windows-Instance, an die Sie den Blockspeicher-Datenträger angehängt haben.



2. Nachdem der browserbasierte SSH-Client verbunden ist, suchen Sie nach Computer Management (Computerverwaltung) in der Windows-Taskleiste, und wählen Sie anschließend Computer Management (Computerverwaltung) aus den Ergebnissen.

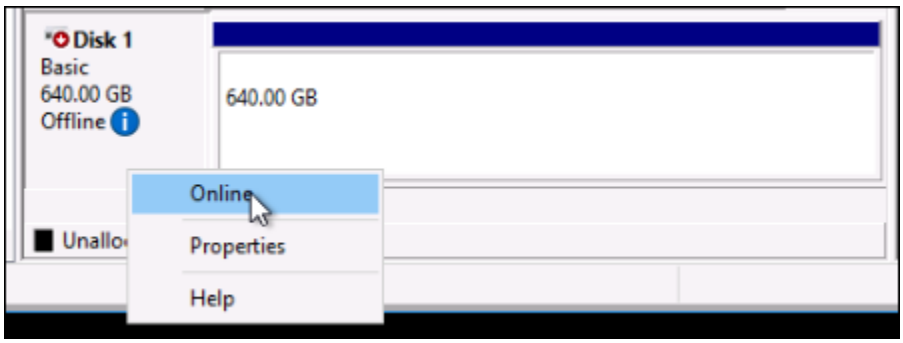


3. Klicken Sie im linken Navigationsmenü der Computer Management (Computerverwaltung)-Konsole auf Disk Management (Festplattenverwaltung), wie im folgenden Beispiel gezeigt.

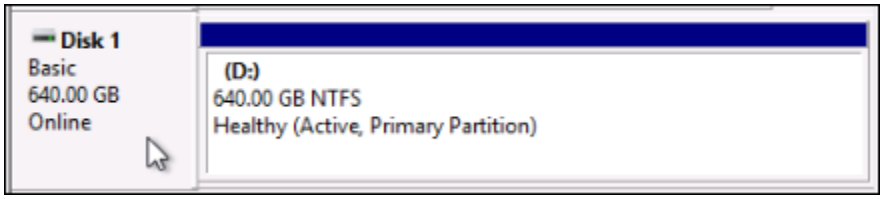


4. Suchen Sie den Datenträger, den Sie vor kurzem an die Instance angehängt haben. Er sollte als „Offline“ gekennzeichnet sein.

5. Klicken Sie mit der rechten Maustaste auf das Label Offline Label, und klicken Sie dann auf Online.



Der Datenträger sollte jetzt mit der Kennzeichnung Online und einem Laufwerkbuchstaben versehen sein. Sie können jetzt auf den Blockspeicher-Datenträger und dessen Inhalte zugreifen. Öffnen Sie den File Explorer und navigieren Sie zu dem gewünschten Laufwerkbuchstaben.

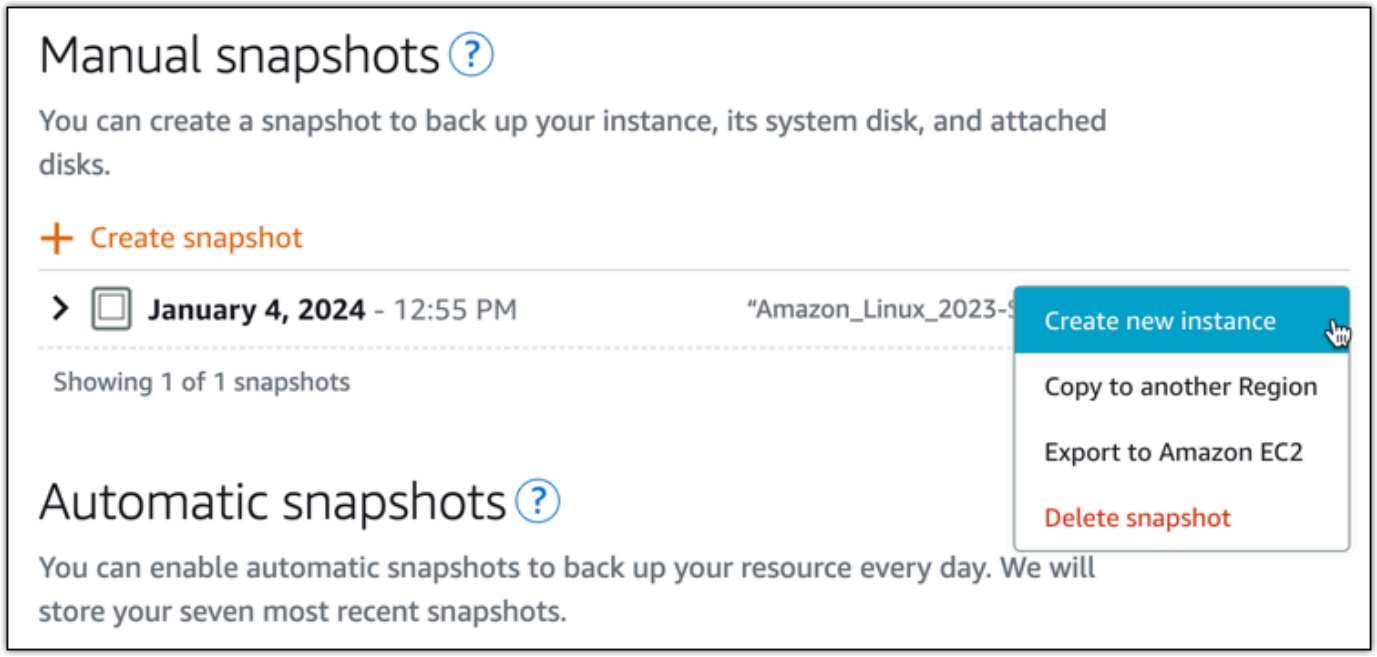


Erstellen einer Lightsail-Instance aus einem Snapshot

Nachdem Sie einen Snapshot in Lightsail erstellt haben, können Sie aus diesem Snapshot eine neue Instance erstellen. Sie können Attribute der neuen Instance ändern, z. B. Instance-Größe und Netzwerktyp – Dual-Stack oder IPv6-only Die neue Instance enthält die Systemfestplatte und die angeschlossenen Blockspeicherfestplatten, die Sie hinzugefügt haben.

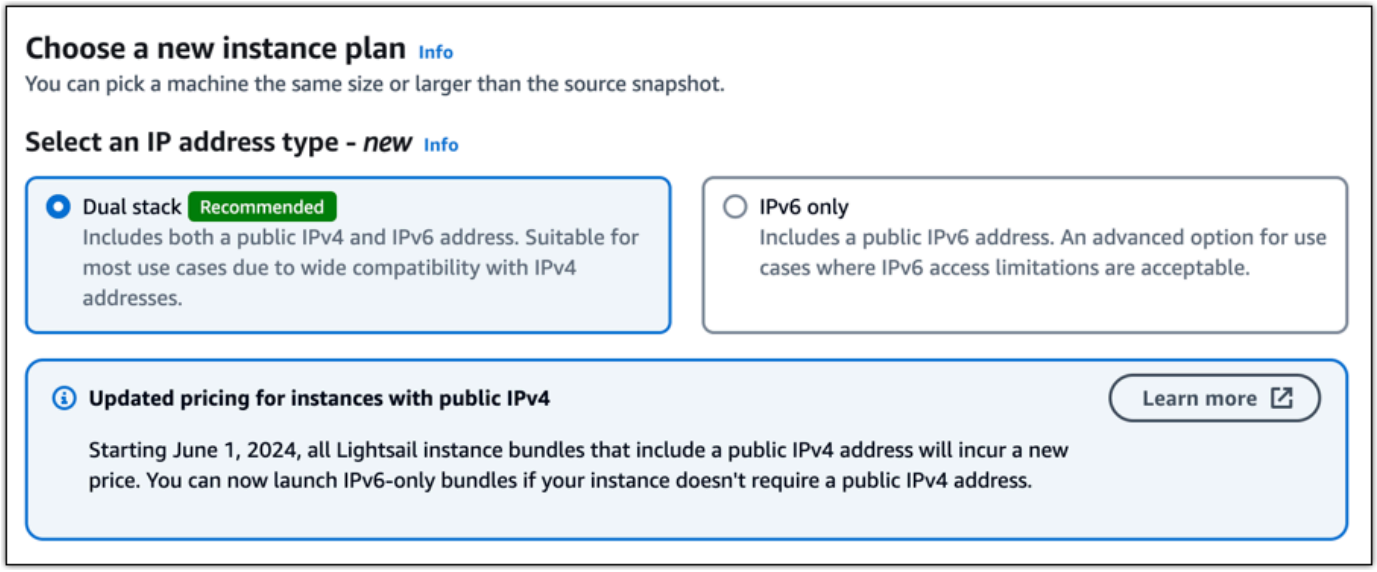
Sie müssen über einen Snapshot einer Instance verfügen, bevor Sie aus diesem Snapshot eine weitere Instance erstellen können. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Linux-/Unix-basierten Lightsail-Instance oder Erstellen eines Snapshots Ihrer Lightsail-Windows Server-Instance.

1. Wählen Sie in der Lightsail-Konsole die Instance aus, für die Sie einen Snapshot erstellen möchten, um eine neue Instance zu erstellen.
2. Wählen Sie die Registerkarte Snapshots aus.
3. Wählen Sie im Abschnitt Manuelle Snapshots das Aktionsmenüsymbol (⋮) neben dem Snapshot und dann Neue Instance erstellen aus.



4. Die Seite Erstellen einer Instance aus einem Snapshot wird geöffnet. Wählen Sie die optionalen Einstellungen aus, die Sie verwenden möchten. Beispielsweise können Sie die Availability Zone ändern, ein Launch-Skript hinzufügenoder die Art und Weise ändern, wie Sie eine Verbindung mit Ihrer Instance herstellen.
5. Wählen Sie einen Plan (oder ein Paket) für Ihre neue Instance aus. Sie können eine Instance erstellen, die einen Dual-Stack-Instance-Plan (IPv4 und IPv6) oder einen IPv6-onlyPlan verwendet. Sie können auch eine größere Bundle-Größe als die der ursprünglichen Instance wählen. Weitere Informationen zu IPv6-onlyPlänen finden Sie unter IPv6-onlyInstance-Pläne in Lightsail.

> **Note**
>
> Sie können keine Instance erstellen, die eine kleinere Bundle-Größe als die der ursprünglichen Instance verwendet.



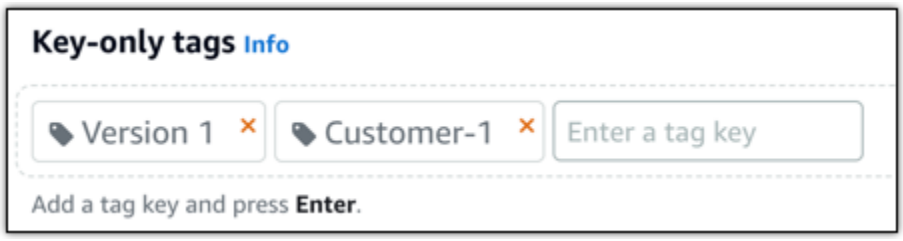
6. Geben Sie einen Namen für Ihre Instance ein.

   Ressourcennamen:

   - Muss innerhalb jedes Ihrer LightsailAWS-Region-Konten eindeutig sein.
   - Muss 2–255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen beginnen und enden.
   - Kann alphanumerische Zeichen, Punkte, Bindestriche und Unterstriche enthalten.

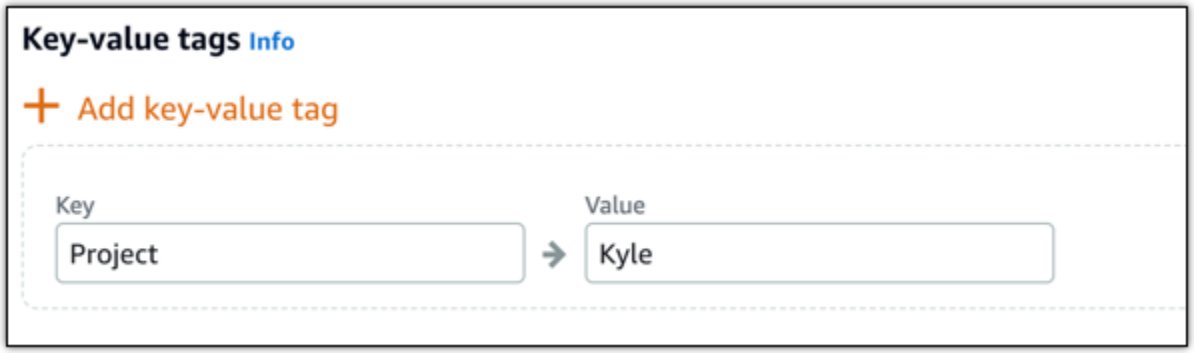
7. Wählen Sie eine der folgenden Optionen, um Ihrer Instance Tags hinzuzufügen:

   - Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihr neues Tag in das Textfeld ein und drücken Sie die Eingabetaste. Wählen Sie Speichern oder Abbrechen aus.

   - Erstellen Sie ein Schlüssel-Wert-Tag und geben Sie dann einen Schlüssel in das Textfeld Schlüssel und einen Wert in das Textfeld Wert ein. Wählen Sie Speichern oder Abbrechen aus.

Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.



> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

8. Wählen Sie Create instance (Instance erstellen).

Lightsail öffnet die Verwaltungsseite, auf der Sie Ihre neue Instance verwalten können.

> **Important**
>
> Benutzerdefinierte Firewall-Regeln von der ursprünglichen Instance werden nicht auf die neue Instance kopiert, die Sie aus einem Snapshot erstellen. Nur die Standardregeln werden auf die neue Instance kopiert. Weitere Informationen finden Sie unter Standard-Instance-Firewall-Regeln weiter unten in diesem Handbuch.

Erstellung einer größeren Instance, eines Blockspeicher-Datenträgers oder einer Datenbank aus einem Lightsail-Snapshot

Es kommt vor. Ihr Cloud-Projekt wächst und Sie benötigen sofort mehr Rechenleistung! Wir können Ihnen weiterhelfen. Erstellen Sie für ein Upsizing Ihrer Lightsail-Instance, Ihres Blockspeicher-Datenträgers oder Ihrer Datenbank einen Snapshot Ihrer Ressource und erstellen Sie dann mithilfe dieses Snapshots eine neue, größere Version dieser Ressource.

> **Note**
>
> Es ist nicht möglich, zum Erstellen einer Ressource aus einem Snapshot eine kleinere Plangröße als die ursprüngliche Ressource zu verwenden. So können Sie beispielsweise nicht von einer 8 GB-Instance zu einer 2 GB-Instance wechseln.
> Die standardmäßige öffentliche IPv4-Adresse, die Ihrer Instance beim Erstellen zugewiesen wird, ändert sich beim Anhalten und Starten Ihrer Instance. Sie können optional eine statische IPv4-Adresse erstellen und an Ihre Instance anfügen. Durch Verwenden einer statischen IP-Adresse können Sie Ausfälle bei Instances oder Software maskieren. Weisen Sie dazu die Adresse einer anderen Instance in Ihrem Konto neu zu. Alternativ können Sie die statische IP-Adresse in einem DNS-Eintrag für Ihre Domain angeben, damit Ihre Domäne auf Ihre Instance verweist. Weitere Informationen finden Sie unter IP-Adressen.

Voraussetzungen

Sie benötigen einen Snapshot Ihrer Lightsail-Instance, Ihres Blockspeicher-Datenträgers oder Ihrer Datenbank. Weitere Informationen finden Sie unter Snapshots.

Erstellen Ihrer Ressource

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie die Registerkarte Snapshots aus.
3. Suchen Sie die Lightsail-Ressource, deren Snapshot Sie verwenden möchten, um eine neue, größere Ressource zu erstellen, und wählen Sie den Rechtspfeil aus, um die Liste der Snapshots zu erweitern.
4. Klicken Sie auf die Auslassungspunkte neben dem Snapshot, den Sie verwenden möchten, und wählen Sie Create new (Neu erstellen) aus.

5. Auf der Seite Create (Erstellen)stehen Ihnen einige optionale Einstellungen zur Auswahl. So können Sie beispielsweise die Availability Zone wechseln. Für Instances können Sie ein Startskript hinzufügen oder den SSH-Schlüssel ändern, mit dem Sie eine Verbindung zu der Instance herstellen.

   Sie können die Standardeinstellungen übernehmen und mit dem nächsten Schritt fortfahren.

6. Wählen Sie den Plan (oder das Bundle) für Ihre neue Ressource aus. An diesem Punkt können Sie gegebenenfalls eine größere Bundle-Größe als die ursprüngliche Ressource auswählen.

   > **Note**
   >
   > Es ist nicht möglich, die Ressource mit einer kleineren Plangröße als die ursprüngliche Ressource zu erstellen. Die Bundle-Optionen, die kleiner als die ursprüngliche Ressource sind, sind nicht verfügbar.

7. Geben Sie einen Namen für Ihre Instance ein.

   Ressourcennamen:

   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

8. Wählen Sie Erstellen aus.

   Lightsail öffnet die Verwaltungsseite für die neue Ressource und Sie können mit der Verwaltung beginnen.

Erstellen einer größeren Lightsail-Instance, eines größeren Blockspeicher-Datenträgers oder einer größeren Datenbank aus einem -Snapshot mithilfe der AWS CLI

Es kommt vor. Ihr Cloud-Projekt wächst und Sie benötigen sofort mehr Rechenleistung! Wir können Ihnen weiterhelfen. Sie können alles innerhalb der Lightsail-Konsole erledigen oder die AWS Command Line Interface (AWS CLI) verwenden.

Wir zeigen Ihnen, wie Sie einen Snapshot Ihrer aktuellen Lightsail-Instance erstellen und eine neue, größere Instance mit der benötigten Rechenleistung basierend auf diesem Snapshot erstellen.

> **Note**
>
> Derzeit gibt es keine Möglichkeit, eine kleinere Instance-Größe (oder Paket) aus einem Snapshot zu erstellen. Sie können nur eine Instance der gleichen Größe oder eine größere Instance erstellen.

Voraussetzungen

1. Falls noch nicht passiert, müssen Sie die AWS CLI installieren. Weitere Informationen finden Sie unter Installieren der AWS Command Line Interface. Achten Sie drauf, die AWS CLI zu konfigurieren.
2. Sie brauchen außerdem einen Snapshot Ihrer Instance, von dem Sie ausgehen können. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Linux- oder Unix-Instance.

Schritt 1: Rufen Sie Ihren Snapshot-Namen ab.

Dies scheint klar, aber Sie müssen Ihren Snapshot-Namen haben, bevor Sie diesen AWS CLI-Befehl ausführen, um die größere Instance zu erstellen. Die gute Nachricht ist, dass das ganz einfach ist.

1. Geben Sie Folgendes in die AWS CLI ein.

   ```
   aws lightsail get-instance-snapshots
   ```

   Die Ausgabe sollte in etwa wie folgt aussehen:

   ```
   {
       "instanceSnapshots": [
           {
               "fromInstanceName": "WordPress-512MB-EXAMPLE",
               "name": "WordPress-512MB-EXAMPLE-system-1234567891011",
               "sizeInGb": 20,
               "resourceType": "InstanceSnapshot",
               "fromInstanceArn":
               "arn:aws:lightsail:us-
   east-1:123456789101:Instance/86f49ee4-26cc-4802-9b0d-12345EXAMPLE",
   ```

```
            "state": "available",
            "arn": "arn:aws:lightsail:us-east-1:123456789101:InstanceSnapshot/
c87acb5f-851e-4fbc-94f1-12345EXAMPLE",
            "fromBundleId": "nano_1_0",
            "fromBlueprintId": "wordpress_4_6_1",
            "createdAt": 1480898073.653,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-east-2"
            }
        }
    ]
}
```

2. Kopieren Sie den Name (Namen)-Wert an eine Stelle, wo Sie ihn später wieder finden. Dies ist der `--instance-snapshot-name`-Wert, den Sie in Ihrem AWS CLI-Befehl verwenden.

Schritt 2: Auswählen eines Bündels

Ein Paket ist nur ein Preismodell und eine Konfiguration für Ihre Instance. Ein Linux-basiertes Medium-Paket kostet beispielsweise 20 USD pro Monat und umfasst 4,0 GB RAM, 80 GB SSD-Speicher usw.

Wenn Sie mit einem kleineren Paket angefangen haben und mehr Rechenleistung benötigen, können Sie ein Upgrade auf ein größeres Paket vornehmen. Weitere Informationen finden Sie unter Erstellen einer größeren Instance, eines Blockspeicher-Datenträgers oder einer Datenbank aus einem Snapshot.

> **Important**
>
> Es ist nicht möglich, eine kleinere Paketgröße anhand eines Snapshots zu erstellen. Wenn Sie ein kleineres Paket erstellen möchten, müssen Sie den Vorgang von vorn ausführen.

1. Geben Sie den folgenden AWS CLI-Befehl ein.

```
aws lightsail get-bundles
```

Die Ausgabe sollte in etwa wie folgt aussehen.

```
{
    "bundles": [
        {
            "name": "Nano",
            "power": 300,
            "price": 5.0,
            "ramSizeInGb": 0.5,
            "diskSizeInGb": 20,
            "transferPerMonthInGb": 1024,
            "cpuCount": 1,
            "instanceType": "t2.nano",
            "isActive": true,
            "bundleId": "nano_1_0"
        },
        {
            "name": "Micro",
            "power": 500,
            "price": 10.0,
            "ramSizeInGb": 1.0,
            "diskSizeInGb": 30,
            "transferPerMonthInGb": 2048,
            "cpuCount": 1,
            "instanceType": "t2.micro",
            "isActive": true,
            "bundleId": "micro_1_0"
        },
        {
            "name": "Small",
            "power": 1000,
            "price": 20.0,
            "ramSizeInGb": 2.0,
            "diskSizeInGb": 40,
            "transferPerMonthInGb": 3072,
            "cpuCount": 1,
            "instanceType": "t2.small",
            "isActive": true,
            "bundleId": "small_1_0"
        },
        {
            "name": "Medium",
            "power": 2000,
            "price": 40.0,
            "ramSizeInGb": 4.0,
```

```
            "diskSizeInGb": 60,
            "transferPerMonthInGb": 4096,
            "cpuCount": 2,
            "instanceType": "t2.medium",
            "isActive": true,
            "bundleId": "medium_1_0"
        },
        {
            "name": "Large",
            "power": 3000,
            "price": 80.0,
            "ramSizeInGb": 8.0,
            "diskSizeInGb": 80,
            "transferPerMonthInGb": 5120,
            "cpuCount": 2,
            "instanceType": "t2.large",
            "isActive": true,
            "bundleId": "large_1_0"
        }
    ]
}
```

2. Suchen Sie den Bundled (Gebündelt)-Wert des gewünschten Pakets. Weitere Informationen finden Sie unter Lightsail- Preise.

Schritt 3: Schreiben Sie Ihren AWS CLI-Befehl und erstellen Sie Ihre neue Instance

Nachdem Sie Ihre Parameterwerte kennen, können Sie den Befehl schreiben und ausführen, um die Instance zu erstellen.

1. Geben Sie Folgendes ein.

```
aws lightsail create-instances-from-snapshot --instance-names
 MyNewInstanceFromSnapshot --availability-zone us-east-1a --instance-snapshot-name
 WordPress-512MB-EXAMPLE-system-1234567891011 --bundle-id medium_1_0
```

Die Ausgabe sollte in etwa wie folgt aussehen.

```
{
    "operations": [
        {
            "status": "Started",
```

```
            "resourceType": "Instance",
            "isTerminal": false,
            "statusChangedAt": 1486863990.961,
            "location": {
                "availabilityZone": "us-east-2a",
                "regionName": "us-east-2"
            },
            "operationType": "CreateInstance",
            "resourceName": "MyNewInstanceFromSnapshot",
            "id": "30fec45e-e7d7-4e18-96c8-12345EXAMPLE",
            "createdAt": 1486863989.784
        }
    ]
}
```


> **Note**
>
> Sie können mit der AWS CLI auch eine Liste der Regionen und Availability Zones zurückgeben. Geben Sie einfach `aws lightsail get-regions --include-availability-zones` ein, um die Liste der Availability Zones für Ihre `get-regions`-Abfrage zurückzugeben.

2. Öffnen Sie nun Ihre neue Instance in der Lightsail-Konsole und beginnen Sie mit den Änderungen.

Nächste Schritte

Nachdem Sie eine neue Instance aus einem Snapshot erstellt haben, können Sie als Nächstes Folgendes erledigen:

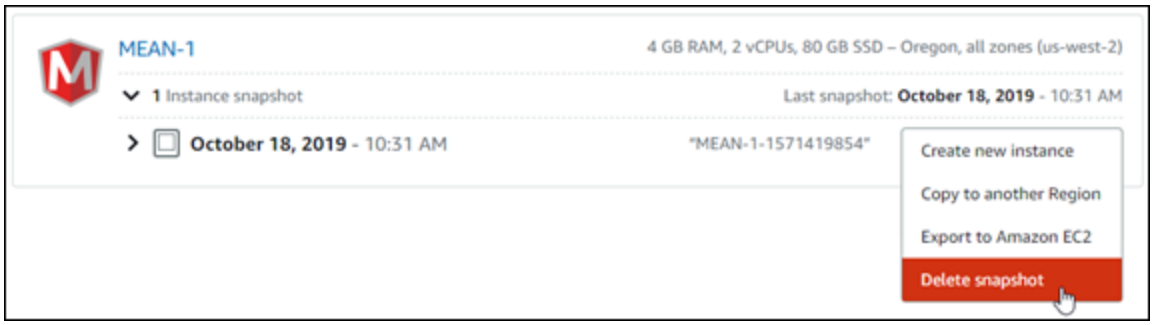
- Wenn Sie die alte Instance nicht mehr brauchen, können Sie sie löschen. Sie können dies mithilfe der Lightsail-Konsole oder mit dem CLI-Befehl delete-instance erledigen.
- Wenn Sie den alten Snapshot nicht mehr brauchen, können Sie ihn löschen. Sie können dies mithilfe der Lightsail-Konsole oder mit dem CLI-Befehl delete-instance-snapshot erledigen.
- Wenn Sie Ihrer alten Instance eine statische IP-Adresse zugewiesen haben, können Sie diese beibehalten und der neuen Instance zuordnen. Dies können Sie über die Konsole erledigen. Siehe Eine statische IP-Adresse erstellen und einer Instance zuordnen.

Lightsail-Snapshots löschen

Löschen Sie Instance-, Datenbank- und Datenträger-Snapshots in Amazon Lightsail, wenn Sie sie nicht mehr benötigen, um eine monatliche Gebühr zu vermeiden.

Löschen eines einzelnen Snapshots

1. Wählen Sie in der Lightsail-Konsole die Registerkarte Snapshots aus.
2. Suchen Sie die Lightsail-Ressource, deren Snapshot Sie löschen möchten, und wählen Sie den Pfeil nach rechts aus, um die Liste der verfügbaren Snapshots für diese Ressource zu erweitern.
3. Wählen Sie das Aktionsmenüsymbol (⋮) neben dem Snapshot aus, den Sie löschen möchten, und wählen Sie dann Delete snapshot (Snapshot löschen) aus.

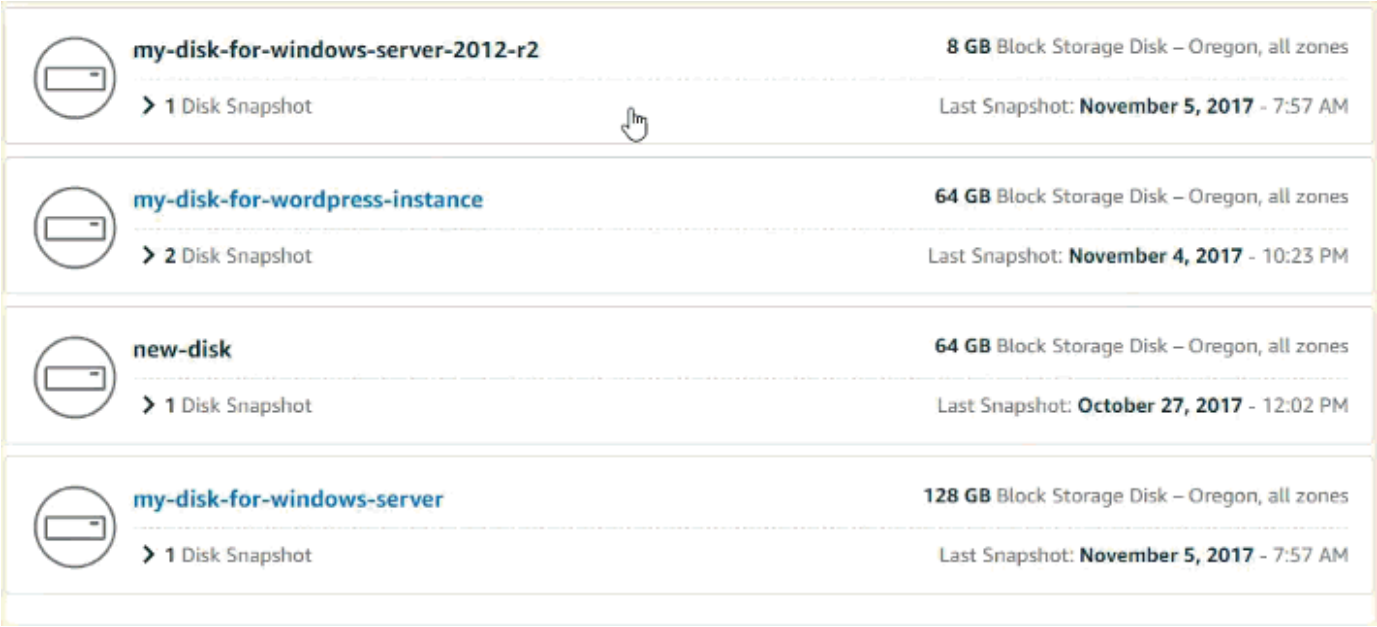


4. Klicken Sie auf Yes (Ja), um zu bestätigen, dass Sie den Snapshot löschen möchten.

> **Important**
>
> Dieser Vorgang ist dauerhaft und kann nicht rückgängig gemacht werden. Sie verlieren alle Daten auf dem Snapshot, wenn Sie ihn löschen.

Löschen mehrerer Snapshots

1. Wählen Sie auf der Lightsail-Startseite Snapshots aus.
2. Suchen Sie die Lightsail-Ressource, deren Snapshots Sie löschen möchten, und wählen Sie den Pfeil nach rechts aus, um die Liste der Snapshots zu erweitern.



3. Wählen Sie Delete multiple (Mehrere löschen) aus.
4. Wählen Sie die Snapshots aus, die Sie löschen möchten, und wählen Sie dann Delete (Löschen) aus.
5. Wählen Sie Yes (Ja) aus, um zu bestätigen, dass Sie die Snapshots löschen möchten.

> **Important**
>
> Dieser Vorgang ist dauerhaft und kann nicht rückgängig gemacht werden. Sie verlieren alle Daten auf den Snapshots, wenn Sie sie löschen.

Automatische Snapshots für Lightsail-Instances und -Festplatten aktivieren oder deaktivieren

Wenn Sie die Feature für automatische Snapshots für eine Instance oder einen Blockspeicher-Datenträger aktivieren, erstellt Amazon Lightsail tägliche Snapshots der Ressource während des Standardzeitpunkts für automatische Snapshots oder eines von Ihnen festgelegten Zeitpunkts. Wie bei einem manuellen Snapshot können Sie einen automatischen Snapshot als Baseline verwenden, um neue Ressourcen zu erstellen oder Datensicherung zu erstellen.

Ihnen wird die Snapshot-Speichergebühr für die automatischen Snapshots in Ihrem Lightsail-Konto in Rechnung gestellt.

Inhalt

Einschränkungen in Bezug auf automatische Snapshots

Die folgenden Einschränkungen gelten in Bezug auf automatische Snapshots:

- Automatische Snapshots können für Blockspeicher-Datenträger mit der Lightsail-Konsole nicht aktiviert oder deaktiviert werden. Zum Aktivieren oder Deaktivieren automatischer Snapshots für Blockspeicher-Datenträger müssen Sie die Lightsail-API, die AWS Command Line Interface (AWS CLI) oder SDKs verwenden. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren automatischer Snapshots mithilfe der AWS CLI.
- Automatische Snapshots werden derzeit nicht für Windows-Instances oder verwaltete Datenbanken unterstützt. Stattdessen müssen Sie manuelle Snapshots Ihrer Windows-Instances oder verwalteten Datenbanken erstellen, um sie zu sichern. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Windows-Server-Instance und Erstellen eines Datenbank-Snapshots. Für verwaltete Datenbanken ist auch die Feature für zeitpunktbezogene Sicherungen standardmäßig aktiviert, mit der Sie Ihre Daten in einer neuen Datenbank wiederherstellen können. Weitere Informationen finden Sie unter Erstellen einer Datenbank aus einer zeitpunktbezogenen Sicherung.
- Automatische Snapshots behalten keine Tags von der Quellressource bei. Um ein Tag von der Quellressource für eine neue Ressource zu behalten, die aus einem automatischen Snapshot erstellt wurde, müssen Sie das Tag manuell hinzufügen, wenn Sie die neue Ressource aus dem automatischen Snapshot erstellen. Weitere Informationen finden Sie unter Hinzufügen von Tags zu einer Ressource.

Aufbewahrung automatischer Snapshots

Die letzten sieben automatischen Snapshots werden gespeichert, bevor der älteste durch den neuesten ersetzt wird. Darüber hinaus werden alle automatischen Snapshots, die einer Ressource zugeordnet sind, gelöscht, wenn Sie die Quellressource löschen. Dieses Verhalten unterscheidet sich

von manuellen Snapshots, die in Ihrem Lightsail-Konto auch nach dem Löschen der Quellressource. Um zu verhindern, dass automatische Snapshots ersetzt oder gelöscht werden, wenn Sie die Quellressource löschen, können Sie Kopieren von automatischen Snapshots als manuellen Snapshot aus.

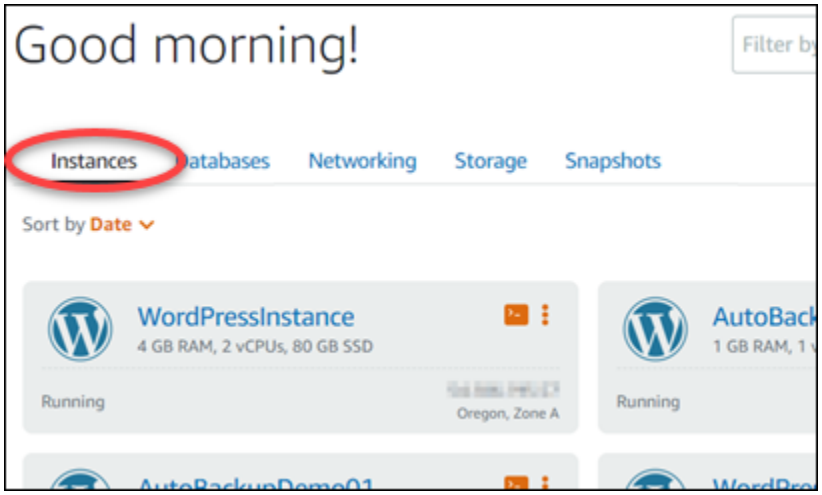
Wenn Sie die Feature für automatische Snapshots für eine Ressource deaktivieren, werden die vorhandenen automatischen Snapshots der Ressource mit der Quellressource so lange aufbewahrt, bis Sie eine der folgenden Aktionen ausführen:

- Aktivieren Sie automatische Snapshots erneut, und die vorhandenen automatischen Snapshots werden durch neuere Snapshots ersetzt.
- Manuelles Löschen der vorhandenen automatischen Snapshots aus.
- Löschen Sie die Quellressource, die die zugeordneten automatischen Snapshots löscht.

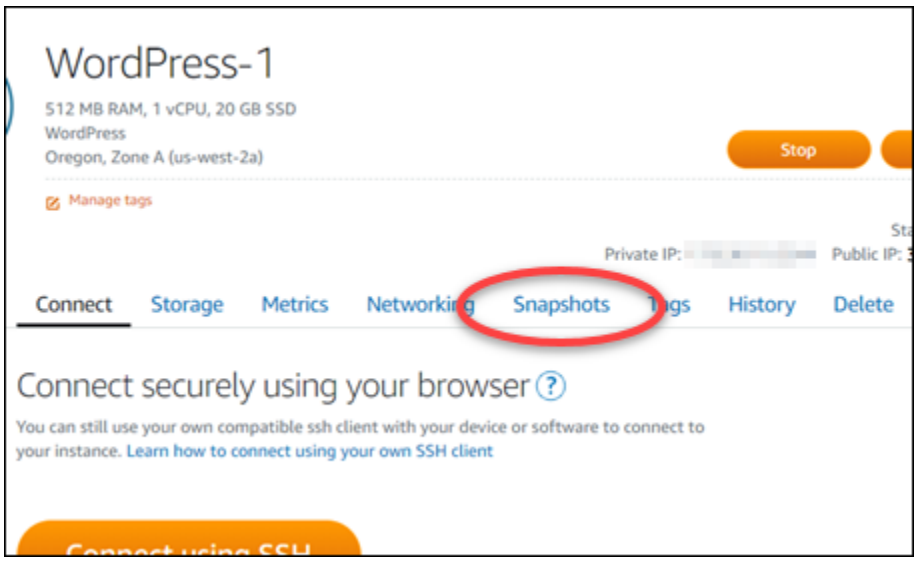
Aktivieren oder Deaktivieren automatischer Snapshots von Instances mithilfe der Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um automatische Snapshots für eine Instance mithilfe der Lightsail-Konsole zu aktivieren oder zu deaktivieren.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Instances.



3. Wählen Sie den Namen der Instance, für die Sie automatische Snapshots aktivieren oder deaktivieren möchten.
4. Wählen Sie auf der Instance-Verwaltungsseite die Registerkarte Snapshots aus.



5. Wählen Sie im Abschnitt Automatic snapshots (Automatische Snapshots) die Option zum Aktivieren aus. Wählen Sie entsprechend die Option zum Deaktivieren, wenn sie aktiviert ist.
6. Wählen Sie an der Eingabeaufforderung Yes, enable (Ja, aktivieren), um automatische Snapshots zu aktivieren, oder Yes, disable (Ja, deaktivieren), um die Feature zu deaktivieren.

   Der automatische Snapshot wird nach einigen Augenblicken aktiviert oder deaktiviert.

   - Wenn Sie die Feature für automatische Snapshots aktiviert haben, können Sie auch den Zeitpunkt für automatische Snapshots ändern. Weitere Informationen finden Sie unter Ändern der automatischen Snapshot-Zeit für Instances oder Blockspeicherdatenträger.
   - Wenn Sie die Feature für automatische Snapshots deaktiviert haben, werden die vorhandenen automatischen Snapshots der Ressource so lange aufbewahrt, bis Sie die Funktion wieder aktivieren und sie durch neue Snapshots ersetzt werden oder bis Sie sie löschen. Ihnen wird die Snapshot-Speichergebühr für die automatischen Snapshots in Ihrem Lightsail-Konto in Rechnung gestellt. Weitere Informationen zum Löschen automatischer Snapshots finden Sie unter Löschen automatischer Snapshots von Instances.

Aktivieren oder Deaktivieren automatischer Snapshots für Instances oder Blockspeicher-Datenträger mithilfe der AWS CLI

Führen Sie die folgenden Schritte aus, um automatische Snapshots für eine Instance oder einen Blockspeicher-Datenträger mithilfe der AWS CLI zu aktivieren oder zu deaktivieren.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.

Falls noch nicht geschehen, installieren Sie die AWS CLI und konfigurieren Sie sie so, dass sie mit Lightsail funktioniert.

2. Geben Sie einen der in diesem Schritt beschriebenen Befehle ein, je nachdem, ob Sie automatische Snapshots aktivieren oder deaktivieren möchten:

> **Note**
>
> Der Parameter `autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}` ist in diesen Befehlen optional. Wenn Sie bei der Aktivierung automatischer Snapshots keinen Zeitpunkt für tägliche automatische Snapshots angeben, weist Lightsail Ihrer Ressource einen Standardzeitpunkt für Snapshots zu. Weitere Informationen finden Sie unter Ändern der automatischen Snapshot-Zeit für Instances oder Blockspeicherdatenträger.

- Geben Sie den folgenden Befehl ein, um automatische Snapshots für eine vorhandene Ressource zu aktivieren:

```
aws lightsail enable-add-on --region Region --resource-name ResourceName --add-
on-request
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
```

  Ersetzen Sie im Befehl Folgendes:

  - *Region* mit der AWS-Region, in der sich die Ressource befindet.
  - *ResourceName* durch den Namen der Ressource.
  - *HH:00* durch die tägliche automatische Snapshot-Zeit in stündlichen Schritten und in koordinierter Weltzeit (UTC).

  Beispiel:

```
aws lightsail enable-add-on --region us-west-2 --resource-name WordPress-1 --add-
on-request
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=18:00}
```

- Geben Sie den folgenden Befehl ein, um automatische Snapshots beim Erstellen einer neuen Instance zu aktivieren:

```
aws lightsail create-instances --region Region --availability-
zone AvailabilityZone --blueprint-id BlueprintID --
bundle-id BundleID --instance-name InstanceName --add-ons
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
```

Ersetzen Sie im Befehl Folgendes:

- *Region* mit der AWS-Region, in der die Instance erstellt werden soll.
- *AvailabilityZone* durch die Availability Zone, in der die Instance erstellt werden soll.
- *BlueprintID* durch die für die Instance zu verwendende Plan-ID.
- *BundleID* durch die Bundle-ID, die für die Instance verwendet werden soll.
- *InstanceName* durch den Namen, der für die Instance verwendet werden soll.
- *HH:00* durch die tägliche automatische Snapshot-Zeit in stündlichen Schritten und in koordinierter Weltzeit (UTC).

Beispiel:

```
aws lightsail create-instances --region us-west-2 --availability-
zone us-west-2a --blueprint-id wordpress_5_1_1_2 --bundle-
id medium_2_0 --instance-name WordPressInstance --add-ons
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=20:00}
```

- Geben Sie den folgenden Befehl ein, um automatische Snapshots beim Erstellen eines neuen Datenträgers zu aktivieren:

```
aws lightsail create-disk --region Region --availability-
zone AvailabilityZone --size-in-gb Size --disk-name DiskName --add-ons
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
```

Ersetzen Sie im Befehl Folgendes:

- *Region* mit der AWS-Region, in der der Datenträger erstellt werden soll.
- *AvailabilityZone* durch die Availability Zone, in der der Datenträger erstellt werden soll.
- *Größe* durch die gewünschte Größe des Datenträgers in GB.
- *DiskName* durch den Namen, der für den Datenträger verwendet werden soll.
- *HH:00* durch die tägliche automatische Snapshot-Zeit in stündlichen Schritten und in koordinierter Weltzeit (UTC).

Beispiel:

```
aws lightsail create-disk --region us-west-2 --availability-
zone us-west-2a --size-in-gb 32 --disk-name Disk01 --add-ons
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=18:59}
```

- Geben Sie den folgenden Befehl ein, um automatische Snapshots für eine Ressource zu deaktivieren:

```
aws lightsail disable-add-on --region Region --resource-name ResourceName --add-
on-type AutoSnapshot
```

Ersetzen Sie im Befehl Folgendes:

- *Region* mit der AWS-Region, in der sich die Ressource befindet.
- *ResourceName* durch den Namen der Ressource.

Beispiel:

```
aws lightsail disable-add-on --region us-west-1 --resource-
name MyFirstWordPressWebsite01 --add-on-type AutoSnapshot
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

Der automatische Snapshot wird nach einigen Augenblicken aktiviert oder deaktiviert.

- Wenn Sie automatische Snapshots aktiviert haben, können Sie auch den Zeitpunkt für automatische Snapshots ändern. Weitere Informationen finden Sie unter Ändern der automatischen Snapshot-Zeit für Instances oder Blockspeicherdatenträger.
- Wenn Sie automatische Snapshots deaktiviert haben, werden die vorhandenen automatischen Snapshots so lange aufbewahrt, bis Sie die Feature wieder aktivieren und sie durch neue Snapshots ersetzt werden oder bis Sie sie löschen. Ihnen wird die Snapshot-Speichergebühr für die automatischen Snapshots in Ihrem Lightsail-Konto in Rechnung gestellt. Weitere Informationen zum Löschen automatischer Snapshots finden Sie unter Löschen automatischer Snapshots von Instances.

> **Note**
>
> Weitere Informationen zu den EnableAddOn- und DisableAddOn-API-Operationen in diesen Befehlen finden Sie unter EnableAddOn und DisableAddOn in der Lightsail-API-Dokumentation.

Ändern der Zeit für automatische Snapshots in Lightsail

Wenn Sie die Feature für automatische Snapshots für eine Instance oder einen Blockspeicher-Datenträger aktivieren, erstellt Lightsail tägliche Snapshots der Ressource während des Standardzeitpunkts für automatische Snapshots oder eines von Ihnen festgelegten Zeitpunkts. Befolgen Sie die Schritte in diesem Handbuch, um den Zeitpunkt für automatische Snapshots für Ihre Ressource zu ändern.

Inhalt

Einschränkungen in Bezug auf den Zeitpunkt für automatische Snapshots

Die folgenden Einschränkungen gelten in Bezug auf den Zeitpunkt für automatische Snapshots

- Der Zeitpunkt für automatische Snapshots kann für Blockspeicher-Datenträger mit der Lightsail-Konsole nicht geändert werden. Zum Ändern des Zeitpunkts für automatische Snapshots für Blockspeicher-Datenträger müssen Sie die Lightsail-API, die AWS Command Line Interface (AWS CLI) oder SDKs verwenden. Weitere Informationen finden Sie unter Ändern des Zeitpunkts für automatische Snapshots mithilfe der AWS CLI.
- Die automatische Snapshot-Zeit kann nur in stündlichen Schritten angegeben werden. Es muss sich auch um eine Uhrzeit handeln, die mehr als 30 Minuten von Ihrer aktuellen Uhrzeit entfernt ist. Der Snapshot wird von Lightsail automatisch zwischen der angegebenen Zeit und bis zu 45 Minuten danach erstellt.

  > **Important**
  >
  > Sie können keine manuellen Snapshots erstellen, wenn ein automatischer Snapshot erstellt wird.

- Wenn Sie den Zeitpukt für automatische Snapshots für eine Ressource ändern, ist dies in der Regel sofort wirksam, außer unter den folgenden Bedingungen:

- Wenn ein automatischer Snapshot für den aktuellen Tag erstellt wurde und Sie den Zeitpunkt für Snapshots in eine spätere Tageszeit ändern, wird der neue Zeitpunkt für Snapshots am folgenden Tag wirksam. Auf diese Weise wird sichergestellt, dass für den aktuellen Tag nicht zwei Snapshots erstellt werden.
- Wenn für den aktuellen Tag noch kein automatischer Snapshot erstellt wurde und Sie den Zeitpunkt für Snapshots in eine frühere Tageszeit ändern, wird der neue Zeitpunkt für Snapshots am folgenden Tag wirksam. Außerdem wird automatisch ein Snapshot zur zuvor festgelegten Zeit für den aktuellen Tag erstellt. Auf diese Weise wird sichergestellt, dass ein Snapshot für den aktuellen Tag erstellt wird.
- Wenn für den aktuellen Tag noch kein automatischer Snapshot erstellt wurde und Sie die Snapshot-Zeit in eine Zeit ändern, die innerhalb von 30 Minuten von der aktuellen Uhrzeit liegt, gilt die neue Snapshot-Zeit ab dem Folgetag. Außerdem wird automatisch ein Snapshot zur zuvor festgelegten Zeit für den aktuellen Tag erstellt. Auf diese Weise wird sichergestellt, dass ein Snapshot für den aktuellen Tag erstellt wird, da mindestens 30 Minuten zwischen der aktuellen Uhrzeit und dem neu festgelegten Zeitpunkt für Snapshots liegen müssen.
- Wenn ein automatischer Snapshot innerhalb von 30 Minuten nach der aktuellen Uhrzeit erstellt werden soll und Sie die Snapshot-Zeit ändern, wird der neue Snapshot-Zeitpunkt am Folgetag wirksam. Außerdem wird automatisch ein Snapshot zur zuvor festgelegten Zeit für den aktuellen Tag erstellt. Auf diese Weise wird sichergestellt, dass ein Snapshot für den aktuellen Tag erstellt wird, da mindestens 30 Minuten zwischen der aktuellen Uhrzeit und dem neu festgelegten Zeitpunkt für Snapshots liegen müssen.

Wenn all diese Bedingungen erfüllt sind, wird in der Lightsail-Konsole die Meldung angezeigt, dass es bis zu 24 Stunden dauern kann, bis der neue Zeitpunkt für Snapshots wirksam wird.

Standardzeitpunkte für automatische Snapshots für AWS-Regionen

Wenn Sie bei der Aktivierung automatischer Snapshots keine automatische Snapshot-Zeit angeben, weist Lightsail eine der folgenden standardmäßigen automatischen Snapshot-Zeiten zu. Die Zeiten hängen von der AWS-Region ab, in der sich Ihre Instance oder der Blockspeicher-Datenträger befindet:

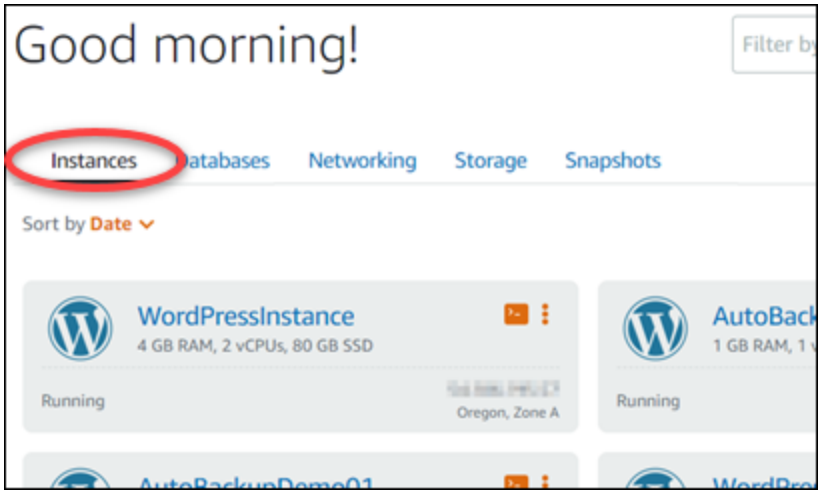
- USA Ost (Ohio) (us-east-2): 03:00 UTC
- USA Ost (Nord-Virginia) (us-east-1): 06:00 UTC
- USA West (Oregon) (us-west-2): 06:00 UTC
- Asien-Pazifik (Mumbai) (ap-south-1): 17:00 UTC

- Asien-Pazifik (Seoul) (ap-northeast-2): 13:00 UTC
- Asien-Pazifik (Singapur) (ap-southeast-1): 14:00 UTC
- Asien-Pazifik (Sydney) (ap-southeast-2): 12:00 UTC
- Asien-Pazifik (Tokio) (ap-northeast-1): 13:00 UTC
- Kanada (Zentral) (ca-central-1): 06:00 UTC
- Europa (Frankfurt) (eu-central-1): 20:00 UTC
- Europa (Irland) (eu-west-1): 22:00 UTC
- Europa (London) (eu-west-2): 06:00 UTC
- Europa (Paris) (eu-west-3): 07:00 UTC
- Europa (Stockholm) (eu-north-1): 08:00 UTC

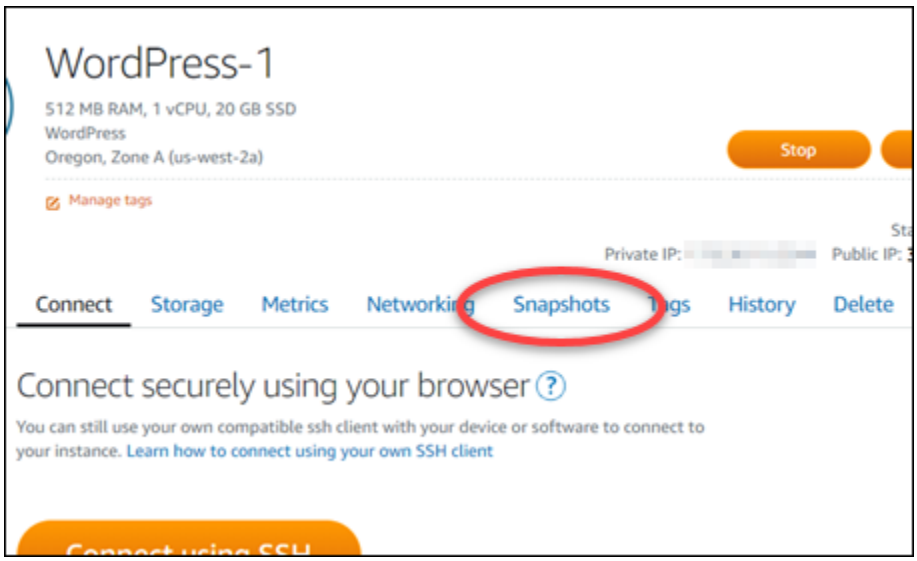
Ändern der automatischen Snapshot-Zeit mithilfe der Lightsail Konsole

Führen Sie die folgenden Schritte aus, um den Zeitpunkt für automatische Snapshots für eine Instance mithilfe der Lightsail-Konsole zu ändern.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Instances.



3. Wählen Sie den Namen der Instance aus, für die Sie den Zeitpunkt für automatische Snapshots ändern möchten.
4. Wählen Sie auf der Instance-Verwaltungsseite die Registerkarte Snapshots aus.



5. Wählen Sie im Abschnitt Automatic snapshots (Automatische Snapshots) die Option Change snapshot time (Zeitpunkt für Snapshots ändern).
6. Wählen Sie eine Tageszeit, zu der Lightsail automatische Snapshots erstellen soll. Die gewählte Uhrzeit muss in koordinierter Weltzeit (Coordinated Universal Time, UTC) angegeben werden.
7. Wählen Sie Change (Ändern), um den neuen Zeitpunkt für automatische Snapshots zu speichern.

   Der Zeitpunkt für automatische Snapshots wird nach wenigen Augenblicken aktualisiert. Für das Datum des Inkrafttretens Ihres neuen Zeitpunkts für automatische Snapshots kann eine Einschränkung gelten. Weitere Informationen finden Sie unter Einschränkungen in Bezug auf den Zeitpunkt für automatische Snapshots.

Ändern des Zeitpunkts für automatische Snapshots für Instances und Blockspeicher-Datenträger mithilfe der AWS CLI

Führen Sie die folgenden Schritte aus, um den Zeitpunkt für automatische Snapshots für eine Instance oder einen Blockspeicher-Datenträger mithilfe der AWS CLI zu ändern.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.

   Falls noch nicht geschehen, installieren Sie die AWS CLI und konfigurieren Sie sie so, dass sie mit Lightsail funktioniert.
2. Geben Sie den folgenden Befehl ein, um den Zeitpunkt für automatische Snapshots für eine Ressource zu ändern:

```
aws lightsail enable-add-on --region Region --resource-name ResourceName --add-on-
request addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
```

Ersetzen Sie im Befehl Folgendes:

- *Region* mit der AWS-Region, in der sich die Ressource befindet.
- *ResourceName* durch den Namen der Ressource.
- *HH:00* durch die tägliche automatische Snapshot-Zeit in stündlichen Schritten und in koordinierter Weltzeit (UTC).

Beispiel:

```
aws lightsail enable-add-on --region us-west-1 --resource-
name MyFirstWordPressWebsite01 --add-on-request
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=12:00}
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

Der Zeitpunkt für automatische Snapshots wird nach wenigen Augenblicken aktualisiert. Für das Datum des Inkrafttretens Ihres neuen Zeitpunkts für automatische Snapshots kann eine Einschränkung gelten. Weitere Informationen finden Sie unter Einschränkungen in Bezug auf den Zeitpunkt für automatische Snapshots.

> **Note**
>
> Weitere Informationen zur EnableAddOn-API-Operation in diesem Befehl finden Sie unter EnableAddOn in der Lightsail-API-Dokumentation.

Löschen automatischer Snapshots in Lightsail

Sie können automatische Snapshots einer Instance oder eines Blockspeicher-Datenträgers in Amazon Lightsail jederzeit löschen, unabhängig davon, ob die Feature aktiviert ist oder ob sie nach der Aktivierung deaktiviert wurde. Ihnen wird die Snapshot-Speichergebühr für die automatischen Snapshots in Ihrem Lightsail-Konto in Rechnung gestellt. Führen Sie die Schritte in diesem Handbuch aus, um automatische Snapshots zu löschen, wenn Sie sie nicht mehr benötigen. Wenn Sie beispielsweise einen automatischen Snapshot in einen manuellen Snapshot kopiert haben und das Original nicht mehr benötigen oder wenn Sie die Feature für automatische Snapshots für Ihre Ressource deaktiviert haben und Sie die vorhandenen automatischen Snapshots, die aufbewahrt wurden, nicht benötigen.

Inhalt

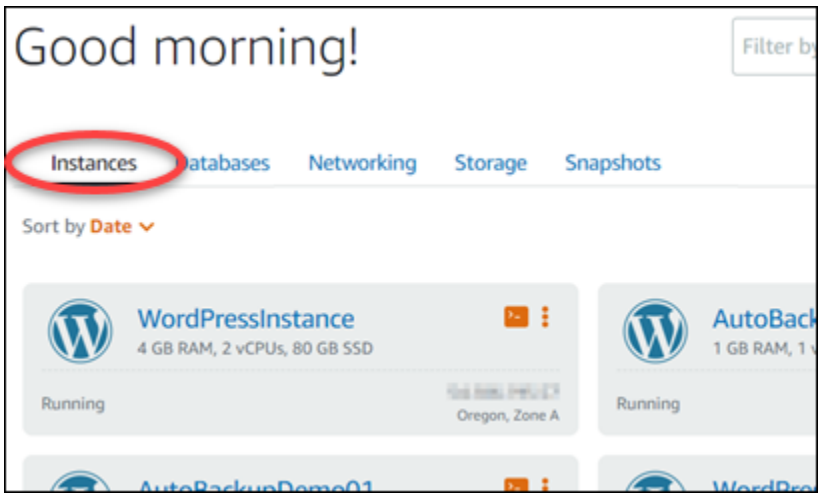
Einschränkung für das Löschen automatischer Snapshots

Automatische Snapshots von Blockspeicher-Datenträgern können nicht mit der Lightsail-Konsole gelöscht werden. Zum Löschen eines automatischen Snapshots eines Blockspeicher-Datenträgers müssen Sie die Lightsail-API, die AWS Command Line Interface (AWS CLI) oder SDKs verwenden. Weitere Informationen finden Sie unter Löschen automatischer Snapshots einer Instance oder eines Blockspeicher-Datenträgers mithilfe der AWS CLI.

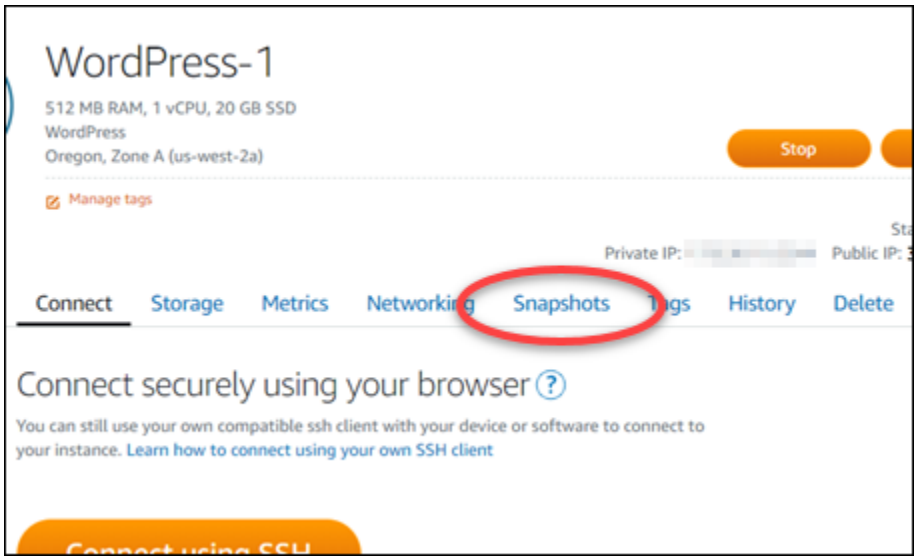
Löschen automatischer Snapshots einer Instance mithilfe der Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um automatische Snapshots einer Instance mithilfe der Lightsail-Konsole zu löschen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Instances.



3. Wählen Sie den Namen der Instance, für die Sie automatische Snapshots löschen möchten.
4. Wählen Sie auf der Instance-Verwaltungsseite die Registerkarte Snapshots aus.



5. Wählen Sie im Abschnitt Automatic snapshots (Automatische Snapshots) das Ellipsensymbol neben dem automatischen Snapshot, den Sie löschen möchten, und klicken Sie dann auf Delete snapshot (Snapshot löschen).
6. Wählen Sie an der Eingabeaufforderung Yes (Ja), um zu bestätigen, dass Sie den Snapshot löschen möchten.

   Der automatische Snapshot wird nach wenigen Augenblicken gelöscht.

Löschen automatischer Snapshots einer Instance oder eines Blockspeicher-Datenträgers mithilfe der AWS CLI

Führen Sie die folgenden Schritte aus, um automatische Snapshots einer Instance oder eines Blockspeicher-Datenträgers mithilfe der AWS CLI zu löschen.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.

   Falls noch nicht geschehen, installieren Sie die AWS CLI und konfigurieren Sie sie so, dass sie mit Lightsail funktioniert.

2. Geben Sie den folgenden Befehl ein, um die Daten der verfügbaren automatischen Snapshots für eine bestimmte Ressource abzurufen. Sie benötigen das Datum des automatischen Snapshots, der als `date`-Parameter im nachfolgenden Befehl angegeben werden soll.

   ```
   aws lightsail --region Region get-auto-snapshots --resource-name ResourceName
   ```

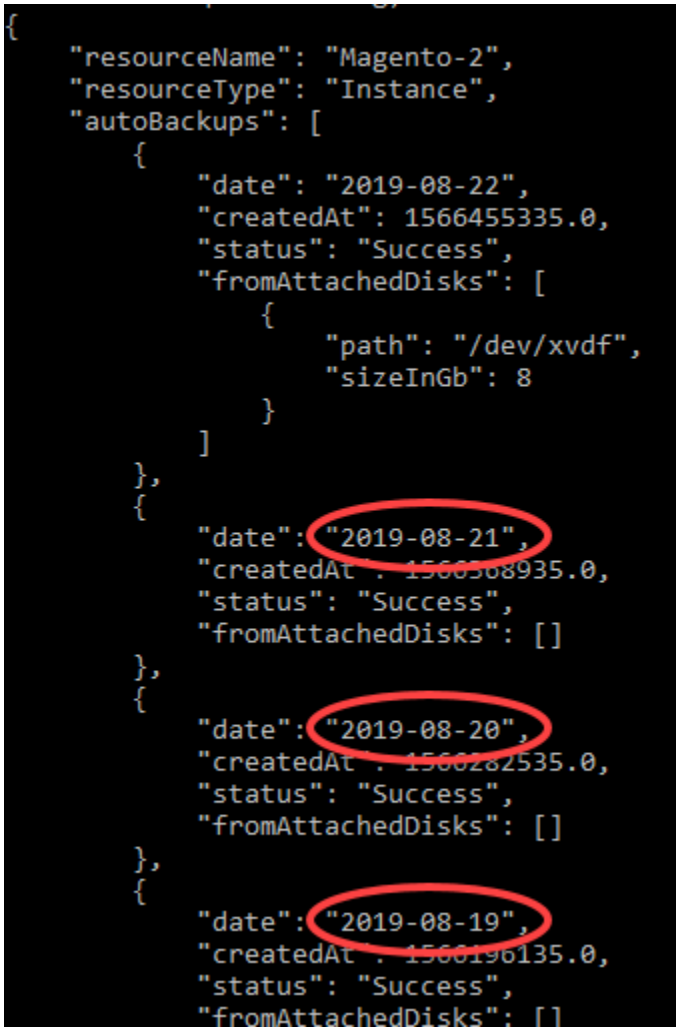
   Ersetzen Sie im Befehl Folgendes:

   - *`Region`* mit der AWS-Region, in der sich die Ressource befindet.
   - *`ResourceName`* durch den Namen der Ressource.

   Beispiel:

   ```
   aws lightsail --region us-west-2 get-auto-snapshots --resource-
   name MyFirstWordPressWebsite01
   ```

   Sie sollten ein Ergebnis ähnlich dem folgenden sehen, das die verfügbaren automatischen Snapshots auflistet:



3. Geben Sie den folgenden Befehl ein, um einen automatischen Snapshot zu löschen:

```
aws lightsail --region Region delete-auto-snapshot --resource-name ResourceName --
date YYYY-MM-DD
```

Ersetzen Sie im Befehl Folgendes:

- *Region* mit der AWS-Region, in der sich die Ressource befindet.
- *ResourceName* durch den Namen der Ressource.
- *JJJJ-MM-TT* durch das Datum des verfügbaren automatischen Snapshots, den Sie anhand des vorhergehenden Befehls erhalten haben.

Beispiel:

```
aws lightsail --region us-west-2 delete-auto-snapshot --resource-
name MyFirstWordPressWebsite01 --date 2019-09-16
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

Der automatische Snapshot wird nach wenigen Augenblicken gelöscht.

> **Note**
>
> Weitere Informationen zu den API-Operationen GetAutoSnapshots und DeleteAutoSnapshot in diesen Befehlen finden Sie unter GetAutoSnapshots und DeleteAutoSnapshot in der Lightsail-API-Dokumentation.

Aufbewahren automatischer Snapshots in Lightsail

Wenn Sie Aktivieren der Feature „Automatische Snapshots“ für eine Instance oder einen Blockspeicher-Datenträger in Amazon Lightsail werden nur die letzten sieben täglichen automatischen Snapshots der Ressource gespeichert. Dann wird der älteste durch den neuesten ersetzt. Darüber hinaus werden alle automatischen Snapshots, die einer Ressource zugeordnet sind, gelöscht, wenn Sie die Quellressource löschen.

Wenn Sie verhindern möchten, dass ein bestimmter automatischer Snapshot ersetzt wird, können Sie ihn als manuellen Snapshot kopieren. Manuelle Snapshots werden so lange aufbewahrt, bis Sie sie manuell löschen.

Befolgen Sie die Schritte in diesem Handbuch, um einen automatischen Snapshot zu speichern, indem Sie ihn als manuellen Snapshot kopieren. Ihnen wird die Snapshot-Speichergebühr für die automatischen Snapshots in Ihrem Lightsail-Konto in Rechnung gestellt.

> **Note**
>
> Wenn Sie die Feature für automatische Snapshots für eine Ressource deaktivieren, werden die vorhandenen automatischen Snapshots der Ressource so lange aufbewahrt, bis Sie die Feature wieder aktivieren und sie durch neuere Snapshots ersetzt werden oder bis Sie die automatischen Snapshots löschen.

Inhalt

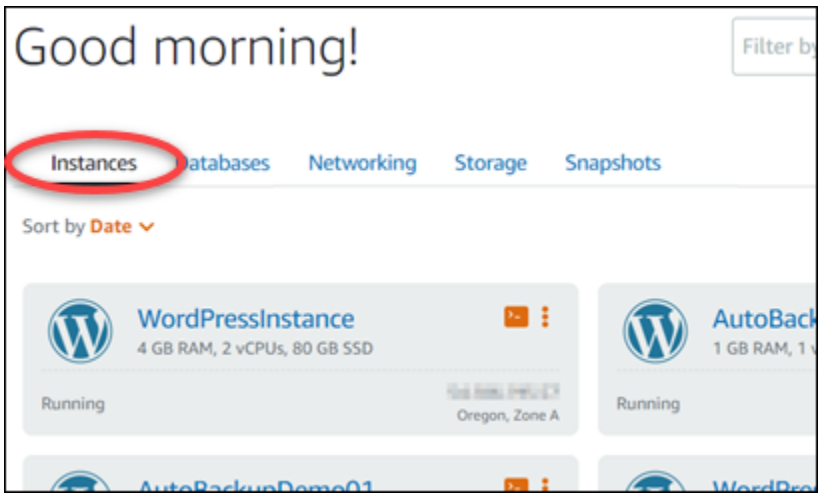
Einschränkung in Bezug auf die Aufbewahrung automatischer Snapshots

Automatische Snapshots von Blockspeicherdatenträgern können nicht mithilfe der Lightsail -Konsole in manuelle Snapshots kopiert werden. Um einen automatischen Snapshot eines Blockspeicherdatenträgers zu kopieren, müssen Sie die Lightsail-API, AWS Command Line Interface (AWS CLI) oder SDKs verwenden. Weitere Informationen finden Sie unter Aufbewahren automatischer Snapshots von Instances und Blockspeicherdatenträgern mithilfe der AWS CLI.

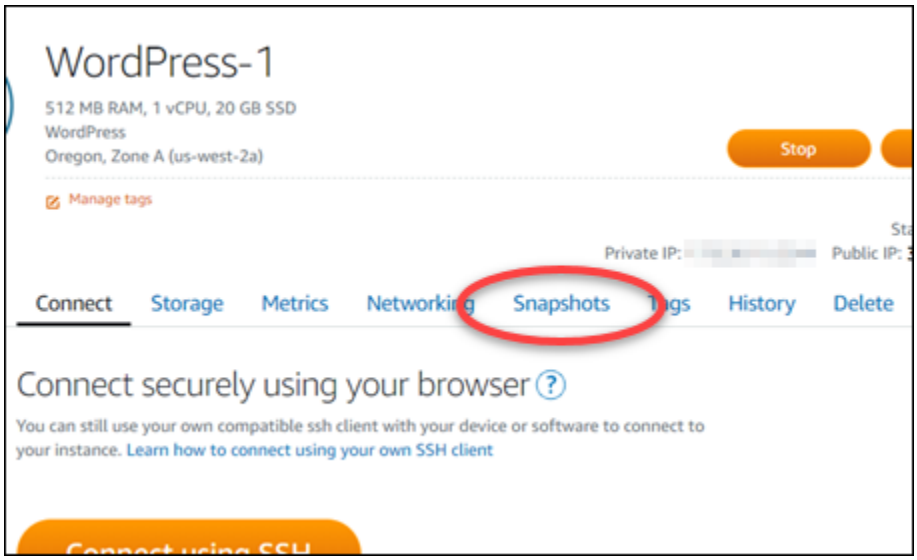
Aufbewahren automatischer Snapshots von Instances mithilfe der Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um automatische Snapshots für eine Instance mithilfe der Lightsail-Konsole beizubehalten.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Instances.



3. Wählen Sie den Namen der Instance aus, für die Sie automatische Snapshots behalten möchten.
4. Wählen Sie auf der Instance-Verwaltungsseite die Registerkarte Snapshots aus.



5. Wählen Sie im Abschnitt Automatic snapshots (Automatische Snapshots) das Ellipsensymbol neben dem automatischen Snapshot aus, den Sie behalten möchten, und klicken Sie dann auf Keep snapshot (Snapshot behalten).
6. Wählen Sie an der Eingabeaufforderung Yes, save (Ja, speichern) aus, um zu bestätigen, dass Sie den automatischen Snapshot behalten möchten.

   Der automatische Snapshot wird nach einigen Momenten als manueller Snapshot kopiert. Manuelle Snapshots werden so lange aufbewahrt, bis Sie sie löschen.

> **Important**
>
> Wenn Sie den automatischen Snapshot nicht mehr benötigen, empfehlen wir Ihnen, ihn zu löschen. Andernfalls wird Ihnen die Snapshot-Speichergebühr für den automatischen Snapshot und den doppelten manuellen Snapshot in Ihrem Lightsail-Konto in Rechnung gestellt. Weitere Informationen finden Sie unter Löschen automatischer Instance-Snapshots.

Aufbewahren automatischer Snapshots von Instances und Blockspeicherdatenträgern mithilfe der AWS CLI

Führen Sie die folgenden Schritte aus, um automatische Snapshots für eine Instance oder einen Blockspeicher-Datenträger mithilfe der AWS CLI aufzubewahren.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.

   Falls noch nicht geschehen, installieren Sie die AWS CLI und konfigurieren Sie sie so, dass sie mit Lightsail funktioniert.

2. Geben Sie den folgenden Befehl ein, um die Daten der verfügbaren automatischen Snapshots für eine bestimmte Ressource abzurufen. Sie benötigen das Datum des automatischen Snapshots, der als `restore date`-Parameter im nachfolgenden Befehl angegeben werden soll.

   ```
   aws lightsail get-auto-snapshots --region Region --resource-name ResourceName
   ```

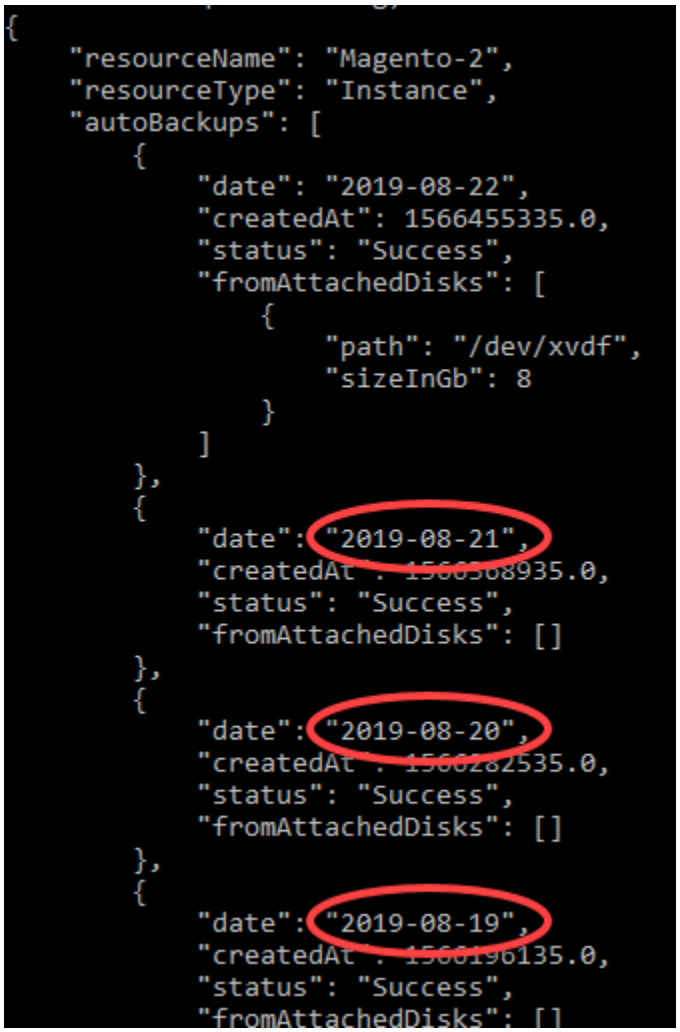
   Ersetzen Sie im Befehl Folgendes:

   - *`Region`* mit der AWS-Region, in der sich die Ressource befindet.
   - *`ResourceName`* durch den Namen der Ressource.

   Beispiel:

   ```
   aws lightsail get-auto-snapshots --region us-west-2 --resource-
   name MyFirstWordPressWebsite01
   ```

Sie sollten ein Ergebnis ähnlich dem folgenden sehen, das die verfügbaren automatischen Snapshots auflistet:



3. Geben Sie den folgenden Befehl ein, um einen automatischen Snapshot für eine bestimmte Ressource beizubehalten:

```
aws lightsail copy-snapshot --region TargetRegion --source-resource-
name ResourceName --restore-date YYYY-MM-DD --source-region SourceRegion --target-
snapshot-name SnapshotName
```

Ersetzen Sie im Befehl Folgendes:

- *TargetRegion* mit der AWS-Region, in die Sie den Snapshot kopieren möchten.
- *ResourceName* durch den Namen der Ressource.

- *JJJJ-MM-TT* durch das Datum des verfügbaren automatischen Snapshots, den Sie anhand des vorhergehenden Befehls erhalten haben.
- *SourceRegion* mit der AWS-Region, in der sich der automatische Snapshot derzeit befindet.
- *SnapshotName* durch den Namen des zu erstellenden neuen Snapshots.

Beispiel:

```
aws lightsail copy-snapshot --region us-west-2 --source-resource-
name MyFirstWordPressWebsite01 --restore-date 2019-09-16 --source-region us-west-2
 --target-snapshot-name Snapshot-Copied-From-Auto-Snapshot
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

Der automatische Snapshot wird nach einigen Momenten als manueller Snapshot kopiert. Manuelle Snapshots werden so lange aufbewahrt, bis Sie sie löschen.

> **Important**
>
> Wenn Sie den automatischen Snapshot nicht mehr benötigen, empfehlen wir Ihnen, ihn zu löschen. Andernfalls wird Ihnen die Snapshot-Speichergebühr für den automatischen Snapshot und den doppelten manuellen Snapshot in Ihrem Lightsail-Konto in Rechnung gestellt. Weitere Informationen finden Sie unter Löschen automatischer Instance-Snapshots.

> **Note**
>
> Weitere Informationen zu den GetAutoSnapshots- und CopySnapshot-API-Operationen in diesen Befehlen finden Sie unter GetAutoSnapshots und CopySnapshot in der Lightsail-API-Dokumentation.

Kopieren von Lightsail-Snapshots von einer AWS-Region in eine andere

Mit Amazon Lightsail können Sie Instance-Snapshots kopieren und Blockspeicher-Datenträger-Snapshots von einer AWS-Region in eine andere oder innerhalb derselben Region kopieren. Kopieren Sie Snapshots zwischen Regionen, wenn Sie Ressourcen in einer Region erstellt und konfiguriert haben, aber später entscheiden, dass eine andere Region besser geeignet ist. Oder, falls Sie Ihre Ressourcen über mehrere Regionen hinweg replizieren möchten. Dieses Handbuch beschreibt den Vorgang des Kopierens von Lightsail-Snapshots.

Voraussetzungen

Erstellen Sie einen Snapshot der zu kopierenden Lightsail-Instance oder des Blockspeicher-Datenträgers. Weitere Informationen finden Sie in einem der folgenden Handbücher:

- Erstellen eines Snapshots Ihrer Linux-/Unix-basierten Instance
- Erstellen eines Snapshots Ihrer Windows Server-Instance
- Erstellen eines Snapshots Ihres Blockspeicherdatenträgers

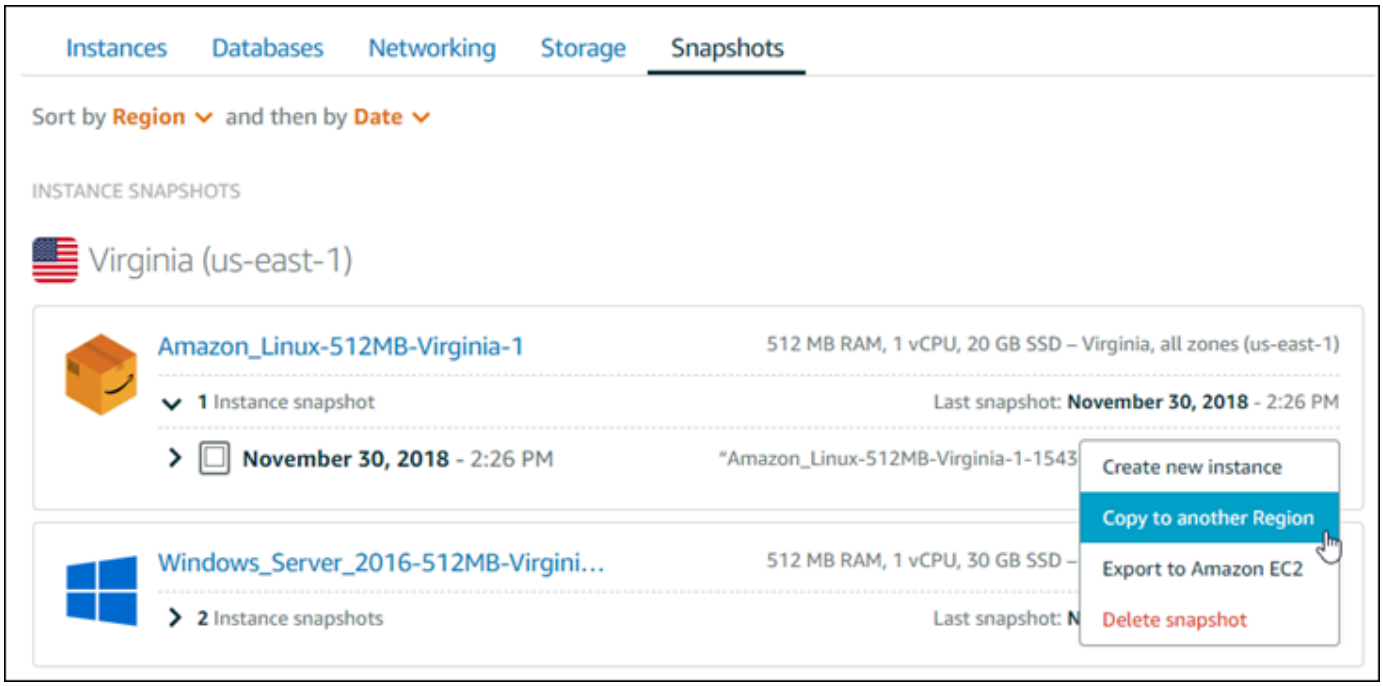
Kopieren eines Snapshots

Sie können Lightsail-Instance-Snapshots und Blockspeicher-Datenträger-Snapshots von einer AWS-Region in eine andere oder innerhalb derselben Region kopieren.

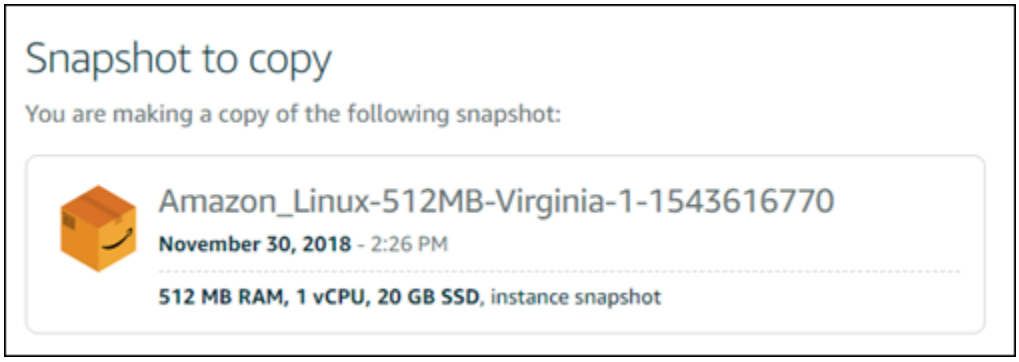
So kopieren Sie einen Lightsail-Snapshot

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Snapshots aus.

3. Suchen Sie die Instance oder den Blockspeicher-Datenträger, die/den Sie kopieren möchten, und erweitern Sie den Knoten, um die verfügbaren Snapshots für diese Ressource anzuzeigen.
4. Wählen Sie das Aktionsmenüsymbol (⋮) für den gewünschten Snapshot und dann Copy to another Region (In eine andere Region kopieren) aus.



5. Vergewissern Sie sich auf der Seite Copy a snapshot (Einen Snapshot kopieren) im Abschnitt Snapshot to copy (Snapshot zum Kopieren), dass die angezeigten Snapshot-Details mit den Spezifikationen der Quell-Instance oder des Quell-Blockspeicher-Datenträgers übereinstimmen.



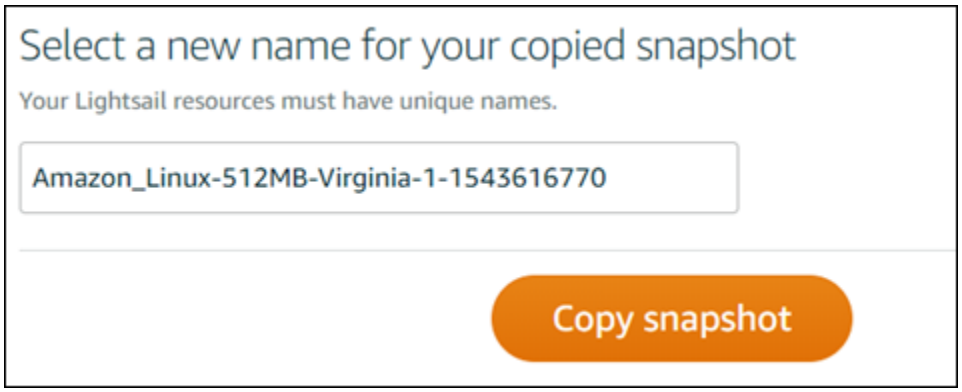
6. Wählen Sie im Abschnitt Select a Region (Eine Region auswählen) auf der Seite die Region für Ihre Snapshot-Kopie aus.
7. Geben Sie einen Namen für Ihre Snapshot-Kopie ein.

   Ressourcennamen:

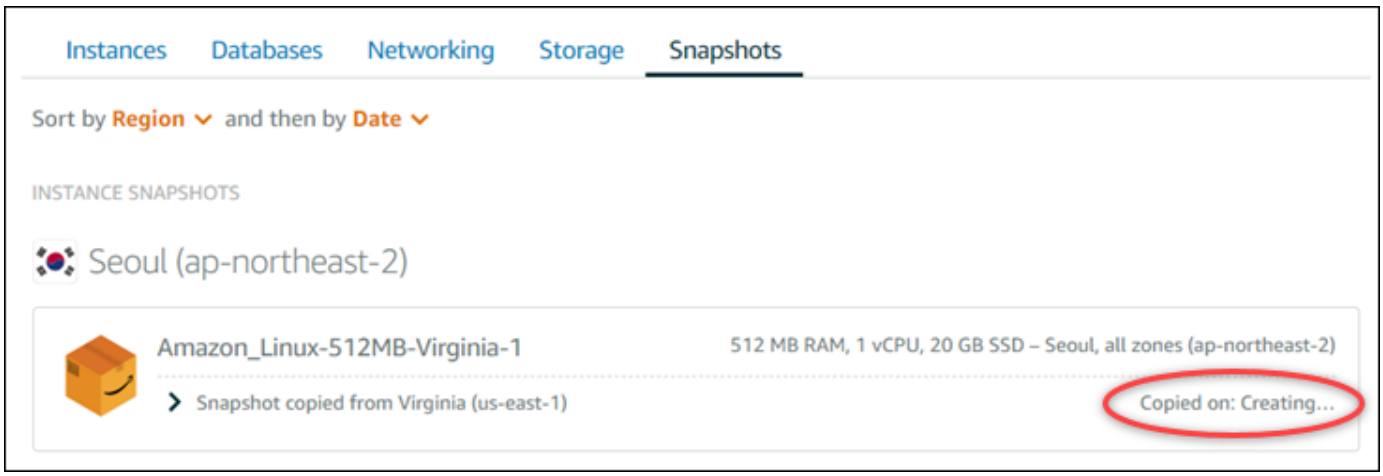
   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.

- Muss zwischen 2 und 255 Zeichen enthalten.
- Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
- Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

8. Wählen Sie Copy Snapshot (Snapshot kopieren) aus.



Ihre Snapshot-Kopie sollte in Kürze verfügbar sein. Dies hängt von der Größe und Konfiguration der Quell-Instance ab. Sie können den Status der Snapshot-Kopie überprüfen, indem Sie zur Registerkarte Snapshots auf der Lightsail-Startseite navigieren und nach dem Snapshot mit dem Status Erstellen suchen, wie im folgenden Screenshot gezeigt. Der Status ändert sich, wenn der Snapshot fertig ist.



Nächste Schritte

Hier sind ein paar zusätzliche Schritte, die Sie durchführen können, nachdem Sie einen Snapshot in Lightsail in eine andere Region kopiert haben:

- Erstellen Sie eine neue Instance aus dem kopierten Snapshot, nachdem er verfügbar ist. Weitere Informationen finden Sie unter Erstellen einer Instance aus einem Snapshot.
- Löschen Sie den Quell--Snapshot, wenn Sie ihn nicht mehr benötigen. Andernfalls wird Ihnen die Speicherung des Snapshots in Rechnung gestellt.

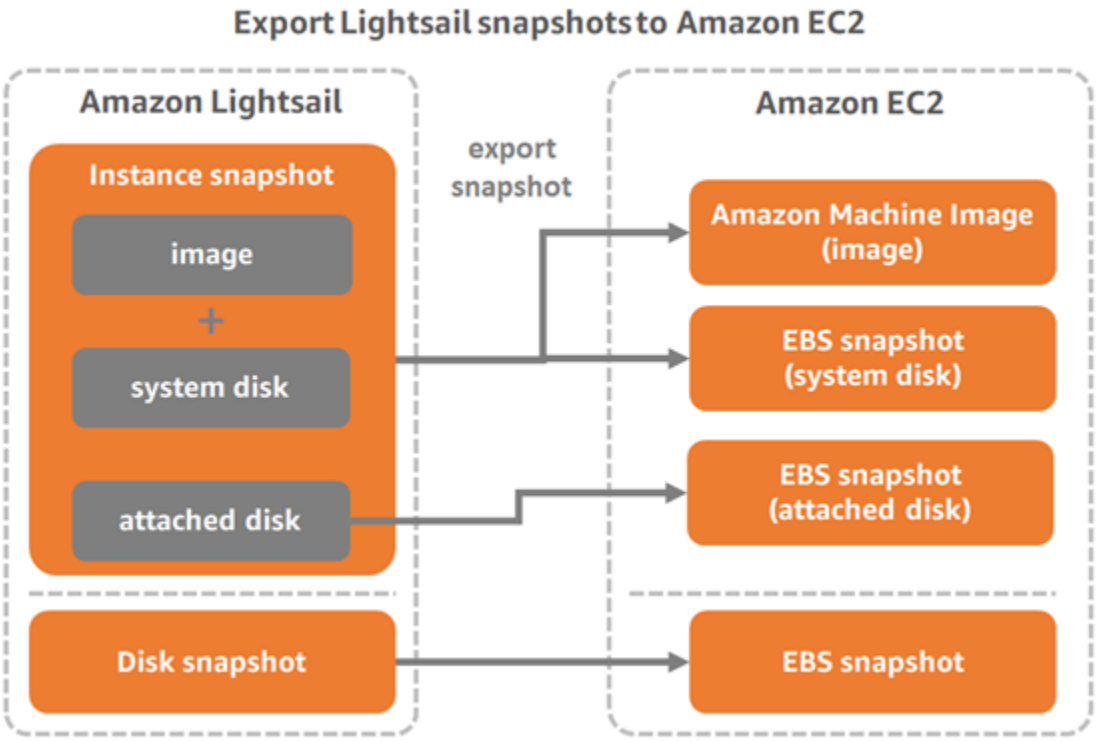
Exportieren von Lightsail-Snapshots nach Amazon EC2

Lightsail-Instance- und Blockspeicherdatenträger-Snapshots können mit einer der folgenden Methoden nach Amazon EC2 exportiert werden:

- Die Lightsail-Konsole. Weitere Informationen finden Sie unter Exportieren von Snapshots nach Amazon EC2.
- Die Lightsail-API AWS Command Line Interface (AWS CLI) oder SDKs. Weitere Informationen finden Sie in ExportSnapshot-Vorgang in der Lightsail-API-Dokumentation oder unter Export-Snapshot-Befehl in der AWS CLI-Dokumentation.

Sie können Instance-Snapshots und Blockspeicherdatenträger-Snapshots exportieren. Snapshots von Django, Ghost und cPanel & WHM-Instances können derzeit jedoch nicht exportiert werden. Snapshots werden in denselben AWS-Region-Bereich von Lightsail nach Amazon EC2 exportiert. Um Snapshots in eine andere Region zu exportieren, kopieren Sie zuerst den Snapshot in eine andere Region in Lightsail und führen Sie dann den Export durch. Weitere Informationen finden Sie unter Kopieren von Snapshots von einer AWS-Region in eine andere.

Der Export eines Lightsail-Instance-Snapshots führt dazu, dass ein Amazon Machine Image (AMI) und ein Amazon Elastic Block Store (Amazon EBS)-Snapshot in Amazon EC2 erstellt werden. Der Grund dafür ist, dass Lightsail-Instances aus einem Image und einem Systemdatenträger bestehen, aber beide in der Lightsail-Konsole als eine Instance zusammengefasst sind, um ihre Verwaltung effizienter zu gestalten. Wenn die Lightsail-Quell-Instance bei der Erstellung des Snapshots mit einem oder mehreren Blockspeicherdatenträger verbunden war, werden zusätzliche EBS-Snapshots für jeden angehängten Datenträger in Amazon EC2 erstellt. Das Exportieren eines Lightsail-Blockspeicher-Datenträger-Snapshots führt dazu, dass in Amazon EC2 ein einzelner EBS-Snapshot erstellt wird. Alle exportierten Ressourcen in Amazon EC2 haben ihre eigenen eindeutigen IDs, die sich von ihren Lightsail-Pendants unterscheiden.



> **Note**
>
> Lightsail verwendet eine AWS Identity and Access Management (IAM)-serviceverknüpfte Rolle (SLR), um Snapshots nach Amazon EC2 zu exportieren. Weitere Informationen zu SLR finden Sie unter Serviceverknüpfte Rollen.

Der Exportvorgang kann einige Zeit in Anspruch nehmen. Dies hängt von der Größe und Konfiguration der Quell-Instance oder des Blockspeicher-Datenträgers ab. Verwenden Sie die Aufgabenüberwachung in der Lightsail-Konsole, um den Status Ihres Exports zu verfolgen. Weitere Informationen finden Sie unter Aufgabenüberwachung.

Erstellung von Amazon-EC2-Ressourcen aus exportierten Lightsail Snapshots

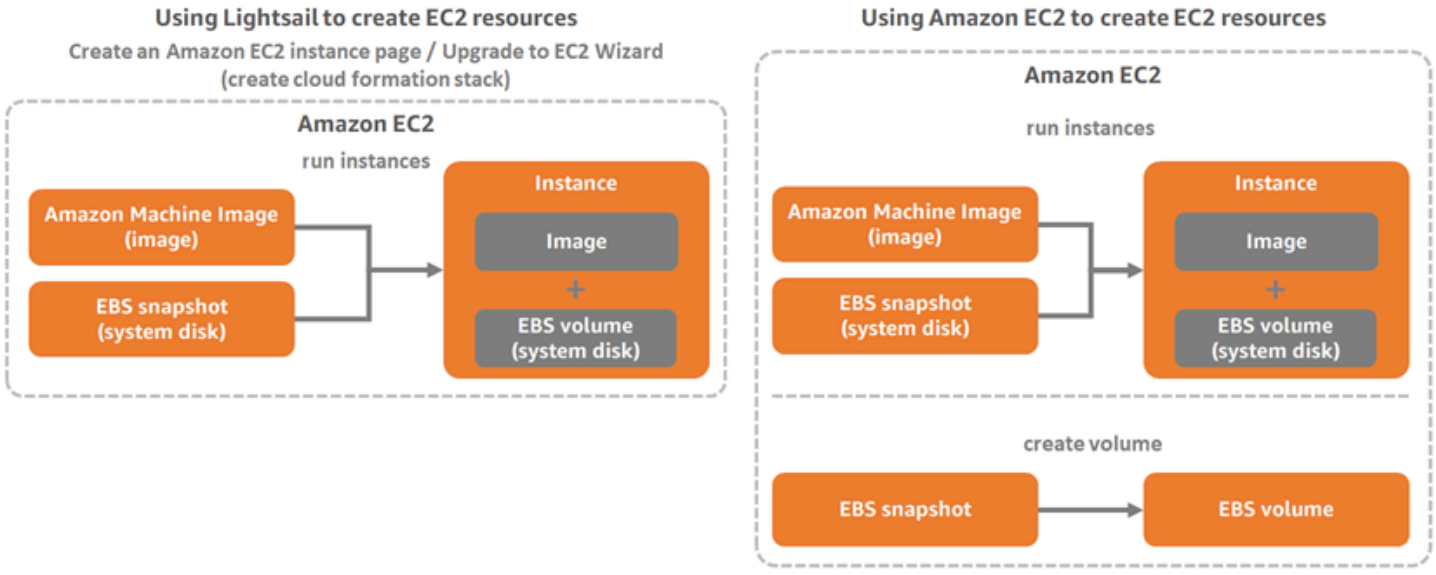
Nachdem ein Lightsail-Snapshot exportiert wurde und in Amazon EC2 verfügbar ist (als AMI, EBS-Snapshot oder beides), können Sie mit einer der folgenden Methoden-Amazon EC2-Ressourcen aus dem Snapshot erstellen:

- Die Seite Erstellen einer Amazon-EC2-Instance in der Lightsail-Konsole, auch bekannt als der Assistent für das Upgrade auf Amazon EC2. Weitere Informationen finden Sie unter Erstellen von Amazon-EC2-Instances aus exportierten Snapshots.
- Die Lightsail-API, AWS CLI oder SDKs. Weitere Informationen finden Sie im CreateCloudFormationStack-Vorgang in der Lightsail-API-Dokumentation oder im create-cloud-formation-stack-Befehl in der AWS CLI-Dokumentation.

> **Note**
>
> Lightsail kann verwendet werden, um Amazon-EC2-Instances aus exportierten Instance-Snapshots zu erstellen, aber es kann nicht verwendet werden, um EBS-Volumes aus exportierten Blockspeicherdatenträger-Snapshots zu erstellen. Dazu müssen Sie die Amazon-EC2-Konsole, die API oder AWS CLI verwenden. Weitere Informationen finden Sie unter Erstellen von Amazon-EC2-Volumes aus exportierten Datenträger-Snapshots.

- Die Amazon-EC2-Konsole, Amazon-EC2-API oder AWS CLI-SDKs. Weitere Informationen finden Sie unter Starten einer Instance mit dem Startassistenten für Instances oder Wiederherstellen eines Amazon-EBS-Volumes aus einem Snapshot in der Amazon-EC2-Dokumentation.

Das Erstellen einer Amazon-EC2-Instance aus einem exportierten Instance-Snapshot (AMI- und EBS-Snapshot) führt zum Starten einer einzelnen EC2-Instance. Der AMI- und EBS-Snapshot, der durch den Export des Lightsail-Instance-Snapshots entstanden ist, wird automatisch mit der EC2-Instance verknüpft. Der exportierte Lightsail-Blockspeicherdatenträger-Snapshot (EBS-Snapshot) kann verwendet werden, um ein EBS-Volume in Amazon EC2 zu erstellen.



> **Note**
>
> Lightsail verwendet einen CloudFormation-Stack, um Instances und die damit verbundenen Ressourcen in EC2 zu erstellen. Weitere Informationen finden Sie unter AWS CloudFormation-Stacks für Lightsail.

Der Prozess zum Erstellen von Amazon-EC2-Ressourcen aus einem exportierten Snapshot kann einige Zeit in Anspruch nehmen. Dies hängt von der Größe und Konfiguration der Quell-Instance ab. Verwenden Sie die Aufgabenüberwachung in der Lightsail-Konsole, um den Status dieser Aufgabe zu verfolgen. Weitere Informationen finden Sie unter Aufgabenüberwachung.

Auswählen eines Amazon-EC2-Instance-Typs

Amazon EC2 bietet eine größere Auswahl an Instance-Optionen als in Lightsail verfügbar sind. In Amazon EC2 können Sie Instance-Typen wählen, die für Datenverarbeitung (C5), den Arbeitsspeicher (R5) oder ein ausgewogenes Verhältnis (T3 und M5) optimiert sind. Lightsail stellt diese Optionen auf der Seite Eine Amazon-EC2-Instance erstellen bereit. Weitere Instance-Typ-Optionen sind jedoch verfügbar, wenn Sie Amazon EC2 verwenden, um neue Instances aus einem exportierten Snapshot zu erstellen. Weitere Informationen zu EC2-Instance-Typen finden Sie unter Instance-Typen in der Amazon-EC2-Dokumentation.

Bevor Sie EC2-Instances aus exportierten Snapshots erstellen, ist es wichtig, die Preisunterschiede zwischen Lightsail und Amazon EC2 zu verstehen. Weitere Informationen über die Preisgestaltung bei Instances finden Sie auf den Seiten Lightsail-Preisgestaltung und Amazon-EC2-Preisgestaltung.

Lightsail und Kompatibilität mit Amazon-EC2-Instance-Typen

Einige Lightsail-Instances sind mit den EC2-Instance-Typ der aktuellen Generation (T3, M5, C5 oder R5) nicht kompatibel, da sie für das erweiterte Netzwerk nicht aktiviert sind. Wenn Ihre Quell-Lightsail-Instance inkompatibel ist, müssen Sie beim Erstellen einer EC2-Instance aus Ihrem exportierten Snapshot einen Instance-Typ der vorherigen Generation (T2, M4, C4 oder R4) auswählen. Diese Optionen werden Ihnen angezeigt, wenn Sie eine EC2-Instance mit der Seite Erstellen einer Amazon-EC2-Instance in der Lightsail-Konsole erstellen.

Um die EC2-Instance-Typen der neuesten Generation zu verwenden, wenn die Quell-Instance Lightsail inkompatibel ist, müssen Sie die neue EC2-Instance mit einem Instance-Typ der vorherigen Generation (T2, M4, C4 oder R4) erstellen, den Netzwerktreiber aktualisieren und die Instance dann

auf den gewünschten Instance-Typ der aktuellen Generation aktualisieren. Weitere Informationen finden Sie unter Amazon-EC2-Instances für erweitertes Netzwerk.

Verbindung zu Amazon-EC2-Instances herstellen

Sie können sich mit Amazon-EC2-Instances so verbinden, wie Sie sich mit Lightsail-Instances verbinden. Das bedeutet, dass SSH für Linux- und Unix-Instances und RDP für Windows-Server-Instances verwendet werden. Der Browser-basierte SSH/RDP-Client, den Sie möglicherweise in der Lightsail-Konsole verwendet haben, ist jedoch je nach verwendeter Browserversion möglicherweise nicht in Amazon EC2 verfügbar, sodass Sie möglicherweise Ihren eigenen SSH/RDP-Client konfigurieren müssen, um eine Verbindung zu Ihren EC2-Instances herzustellen. Weitere Informationen finden Sie in den folgenden Anleitungen:

- Verbinden mit einer Amazon-EC2-Linux- oder Unix-Instance, die aus einem Lightsail-Snapshot erstellt wurde
- Verbinden mit einer Instance von Amazon EC2 Windows Server, die aus einem Lightsail-Snapshot erstellt wurde

Sicherung einer Amazon-EC2-Instance

Nachdem Sie eine EC2-Instance aus einem exportierten Lightsail-Snapshot erstellt haben, müssen Sie möglicherweise einige Aktionen durchführen, um die Sicherheit Ihrer neuen Instances zu verbessern. Die Aktionen sind je nach dem Betriebssystem Ihrer EC2-Instance unterschiedlich.

Sichern von Linux- und Unix-Instances in Amazon EC2

Wenn Sie eine Linux- oder Unix-Instance in Amazon EC2 aus einem exportierten Snapshot mit EC2 (die EC2-Konsole, die EC2-API, die AWS CLI für EC2 oder SDKs für EC2) erstellen, kann die neue EC2-Instance dauerhafte SSH-Schlüssel vom Lightsail-Service enthalten. Wir empfehlen, diese Schlüssel zu entfernen, um die neue Instance besser zu sichern.

Weitere Informationen finden Sie unter Sichern einer Amazon-EC2-Linux- oder Unix-Instance, die aus einem Lightsail-Snapshot erstellt wurde.

Sichern von Windows-Server-Instances in Amazon EC2

Nachdem Sie aus einem exportierten Snapshot eine Windows-Server-Instance in Amazon EC2 erstellt haben, kann jeder Benutzer in Ihrem AWS-Konto mit Zugriff auf Lightsail und EC2 das der

Quell-Instance zuerst zugewiesene Standard-Administratorpasswort abrufen, das auch das Passwort für die neue EC2-Instance ist. Um die Sicherheit zu erhöhen, empfehlen wir Ihnen, das Standard-Administratorpasswort für Ihre Amazon-EC2-Instance zu ändern, falls Sie dies noch nicht getan haben.

Weitere Informationen finden Sie unter Sichern einer Instance von Amazon EC2 Windows Server, die aus einem Lightsail-Snapshot erstellt wurde.

Lightsail Snapshots exportieren und Ressourcen in Amazon EC2 erstellen

Um mit dem Exportieren von Snapshots und dem Erstellen von Amazon-EC2-Ressourcen aus diesen zu beginnen, lesen Sie die folgenden Anleitungen:

- Aufgabenüberwachung
- AWS CloudFormation-Stacks für Lightsail
- Exportieren von Snapshots nach Amazon EC2
- Erstellen von Amazon-EC2-Instances aus exportierten Snapshots
- Erstellen von Amazon-EBS-Volumes aus exportierten Datenträger-Snapshots
- Erweitertes Netzwerk für Amazon-EC2-Instances
- Verbinden mit einer Amazon-EC2-Linux- oder Unix-Instance, die aus einem Lightsail-Snapshot erstellt wurde
- Verbinden mit einer Instance von Amazon EC2 Windows Server, die aus einem Lightsail-Snapshot erstellt wurde
- Sichern einer Amazon-EC2-Linux- oder Unix-Instance, die aus einem Lightsail-Snapshot erstellt wurde
- Sichern einer Instance von Amazon EC2 Windows Server, die aus einem Lightsail-Snapshot erstellt wurde
- Kopieren von Snapshots von einer AWS-Region in eine andere
- Service-verknüpfte Rollen

Exportieren von Lightsail-Snapshots nach Amazon EC2

Sie können Amazon Lightsail-Instance- und Block-Snapshots nach Amazon Elastic Compute Cloud (Amazon EC2) exportieren. Der Export eines Lightsail-Instance-Snapshots führt dazu, dass

ein Amazon Machine Image (AMI) und ein Amazon Elastic Block Store (Amazon EBS)-Snapshot in Amazon EC2 erstellt werden. Der Grund dafür ist, dass Lightsail-Instances aus einem Image und einem Systemdatenträger bestehen, aber beide in der Lightsail-Konsole als eine Instance zusammengefasst sind, um ihre Verwaltung effizienter zu gestalten. Wenn die Lightsail-Quell-Instance bei der Erstellung des Snapshots mit einem oder mehreren Blockspeicher-Datenträgern verbunden ist, werden zusätzliche EBS-Snapshots für jeden angehängten Datenträger in Amazon EC2 erstellt.

Das Exportieren eines Lightsail-Blockspeicher-Datenträger-Snapshots führt dazu, dass in Amazon EC2 ein einzelner EBS-Snapshot erstellt wird. Alle exportierten Ressourcen in Amazon EC2 haben ihre eigenen eindeutigen IDs, die sich von ihren Lightsail-Pendants unterscheiden.

Dieses Handbuch beschreibt, wie Sie einen Lightsail-Snapshot exportieren, den Status Ihres Exports verfolgen und die nächsten Schritte nach der Verfügbarkeit des exportierten Snapshots in Amazon EC2 (als AMI-, EBS-Snapshot oder beides) durchführen.

> **Important**
>
> Wir empfehlen, dass Sie sich mit dem Lightsail-Exportprozess vertraut machen, bevor Sie die Schritte in diesem Handbuch durchführen. Weitere Informationen finden Sie unter Exportieren von Snapshots nach Amazon EC2.

Inhalt

Serviceverknüpfte Rolle und erforderliche IAM-Berechtigungen für den Export von Lightsail-Snapshots

Lightsail verwendet eine AWS Identity and Access Management (IAM)-serviceverknüpfte Rolle (SLR), um Snapshots nach Amazon EC2 zu exportieren. Weitere Informationen zu SLR finden Sie unter Serviceverknüpfte Rollen.

Die folgenden zusätzlichen Berechtigungen müssen möglicherweise in IAM konfiguriert werden, je nachdem, welcher Benutzer den Snapshot-Export durchführen soll:

- Wenn der Amazon-Konto-Stammbenutzer den Export durchführen soll, fahren Sie mit dem Abschnitt Voraussetzungen in diesem Handbuch fort. Der Stammbenutzer verfügt bereits über die erforderlichen Berechtigungen, um den Snapshot-Export durchzuführen.
- Wenn ein IAM-Benutzer den Export durchführt, muss ein AWS-Kontoadministrator dem Benutzer die folgende Richtlinie hinzufügen. Weitere Informationen zum Ändern von Berechtigungen für einen Benutzer finden Sie unter Ändern von Berechtigungen für einen IAM-Benutzer in der IAM-Dokumentation.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
lightsail.amazonaws.com/AWSServiceRoleForLightsail*",
            "Condition": {"StringLike": {"iam:AWSServiceName":
 "lightsail.amazonaws.com"}}
        },
        {
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
lightsail.amazonaws.com/AWSServiceRoleForLightsail*"
        }
    ]
}
```

Voraussetzungen

Erstellen Sie einen Snapshot der Lightsail-Instance oder des Blockspeicher-Datenträgers für den Export nach Amazon EC2. Weitere Informationen finden Sie in einem der folgenden Handbücher:

- Erstellen eines Snapshots Ihrer Linux-/Unix-basierten Instance
- Erstellen eines Snapshots Ihrer Windows Server-Instance
- Erstellen eines Snapshots Ihres Blockspeicherdatenträgers

Einen Lightsail-Snapshot nach Amazon EC2 exportieren

Der effizienteste Weg, einen Snapshot nach Amazon EC2 zu exportieren, ist die Verwendung der Lightsail-Konsole. Sie können Snapshots auch über die Lightsail-API, AWS Command Line Interface (AWS CLI) oder SDKs exportieren. Weitere Informationen finden Sie in ExportSnapshot-Vorgang in der Lightsail-API-Dokumentation oder unter Export-Snapshot-Befehl in der AWS CLI-Dokumentation.

> **Note**
>
> Snapshots werden in denselben AWS-Region-Bereich von Lightsail nach Amazon EC2 exportiert. Um Snapshots in eine andere Region zu exportieren, kopieren Sie zuerst den Snapshot in eine andere Region in Lightsail und führen Sie dann den Export durch. Weitere Informationen finden Sie unter Kopieren von Snapshots von einer AWS-Region in eine andere.

Wie Sie einen Lightsail-Snapshot nach Amazon EC2 exportieren

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite Snapshots aus.
3. Suchen Sie die Instance oder den Blockspeicher-Datenträger für den Export und erweitern Sie den Knoten, um die verfügbaren Snapshots für diese Ressource anzuzeigen.
4. Wählen Sie das Menü Aktion für den gewünschten Snapshot und dann Export nach Amazon EC2 aus.

> **Note**
>
> Snapshots von cPanel und WHM, Django und Ghost-Instances können derzeit nicht nach Amazon EC2 exportiert werden.

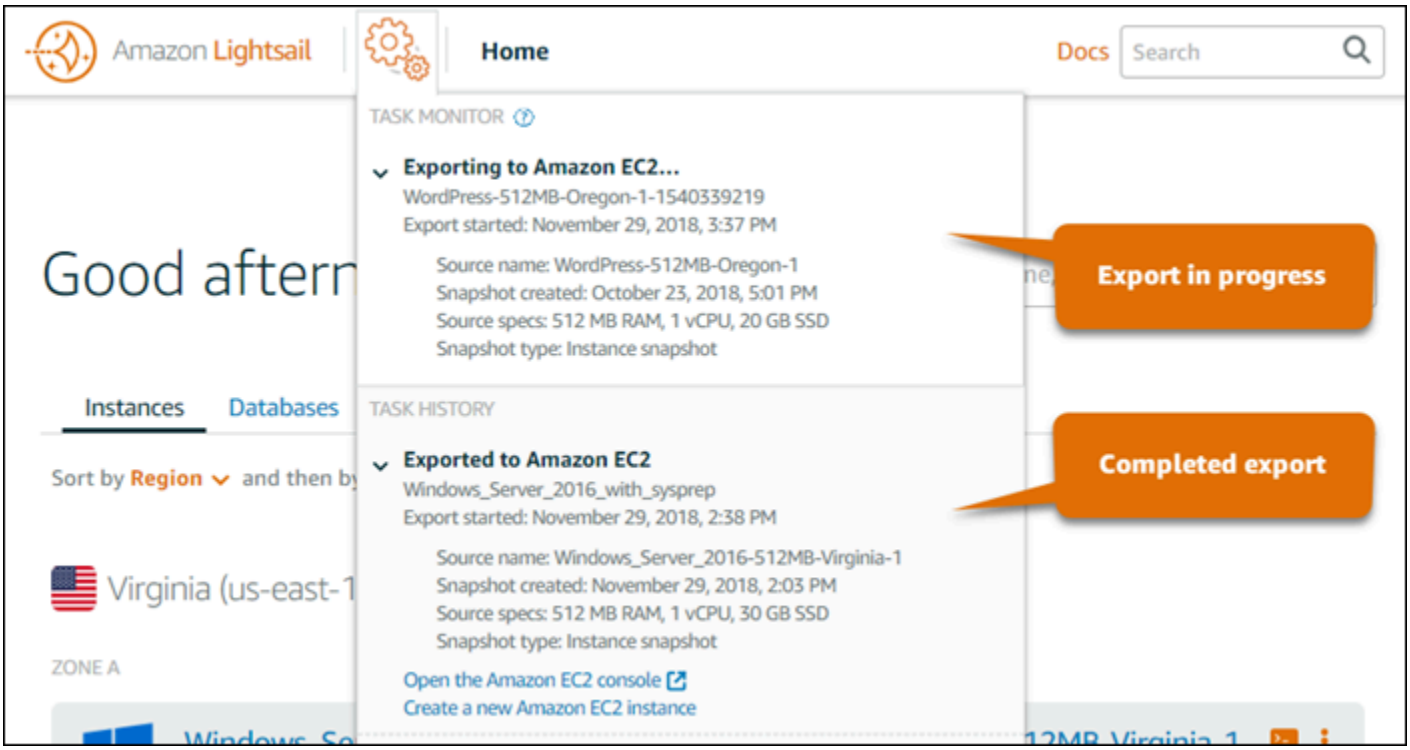
5. Überprüfen Sie die wichtigen Details, die in der Eingabeaufforderung angezeigt werden.
6. Wenn Sie mit dem Export nach Amazon EC2 einverstanden sind, wählen Sie Ja, weiter aus, um den Prozess zu starten.

   Der Exportvorgang kann einige Zeit in Anspruch nehmen. Dies hängt von der Größe und Konfiguration der Quell-Instance oder des Blockspeicher-Datenträgers ab. Fahren Sie mit dem Abschnitt Verfolgen des Status Ihres Exports in diesem Handbuch fort, um den Status Ihres Exports zu verfolgen.

Verfolgen des Status Ihres Exports

Verwenden Sie die Aufgabenüberwachung in der Lightsail-Konsole, um den Status Ihres Exports zu verfolgen. Er ist über den oberen Navigationsbereich auf allen Seiten der Lightsail-Konsole zugänglich. Weitere Informationen finden Sie unter Aufgabenüberwachung.

Die folgenden Informationen werden in der Aufgabenüberwachung für Snapshot-Exports angezeigt:



- Snapshot-Name – Der Name des Quell-Lightsail-Snapshots.
- Export gestartet – Datum und Uhrzeit, zu der der Snapshot-Export gestartet wurde.
- Snapshot erstellt – Das Datum und die Uhrzeit, zu der der Quell-Lightsail-Snapshot erstellt wurde.

- Quellspezifikationen – Die Spezifikationen der Lightsail-Quell-Instance (z. B. Speicher, Verarbeitung und Speicherung).
- Snapshot-Typ – Der Typ des Lightsail-Snapshots. Es handelt sich entweder um einen Instance-Snapshot oder einen Datenträger-Snapshot.

Die folgenden Informationen werden in der Aufgabenüberwachung für abgeschlossene Snapshot-Exports angezeigt:

- Exportiert wird angezeigt, wenn der Snapshot erfolgreich nach Amazon EC2 exportiert wurde.
- Failed wird angezeigt, wenn es ein Problem beim Export des Snapshots gab.

Wenn der Snapshot erfolgreich exportiert wurde, zeigt die Aufgabenüberwachung die folgenden Optionen für den abgeschlossenen Export an:

- Eine neue Amazon-EC2-Instance erstellen – Wählen Sie diese Option, um eine neue Instance in Amazon EC2 über die Lightsail-Konsole zu erstellen. Weitere Informationen finden Sie unter Erstellen von Amazon-EC2-Instances aus exportierten Snapshots.
- Öffnen der Amazon-EC2-Konsole – Wählen Sie diese Option aus, um die Amazon-EC2-Konsole zu verwenden, um neue EC2-Ressourcen aus Ihrem exportierten Snapshot zu erstellen. Wenn Sie einen Lightsail-Blockspeicher-Datenträger-Snapshot exportiert haben, müssen Sie mit Amazon EC2 ein EBS-Volume aus dem Snapshot erstellen (einen EBS-Snapshot). Weitere Informationen finden Sie unter Starten einer Instance mit dem Startassistenten für Instances oder Wiederherstellen eines Amazon-EBS-Volumes aus einem Snapshot in der Amazon-EC2-Dokumentation.

> **Note**
>
> Löschen Sie den Quell-Lightsail-Snapshot, wenn Sie ihn nicht mehr benötigen. Andernfalls wird Ihnen die Speicherung in Rechnung gestellt.

Amazon EBS-Volumes aus exportierten Lightsail-Festplatten-Snapshots erstellen

Nachdem ein Lightsail-Blockspeicherdatenträger-Snapshot exportiert wurde und in Amazon EC2 (als EBS-Snapshot) verfügbar ist, können Sie über die Amazon-EC2-Konsole ein EBS-Volumen aus dem Snapshot erstellen.

> **Note**
>
> Um EC2-Instances aus exportierten Instance-Snapshots zu erstellen, lesen Sie Erstellen von Amazon-EC2-Instances aus exportierten Snapshots in Lightsail.

Sie können neue EBS-Volumes außerdem über die Amazon-EC2-API, AWS CLI oder SDKs erstellen. Weitere Informationen finden Sie unter Starten einer Instance mit dem Startassistenten für Instances oder Wiederherstellen eines Amazon-EBS-Volumes aus einem Snapshot in der Amazon-EC2-Dokumentation.

> **Important**
>
> Wir empfehlen, dass Sie sich mit dem Lightsail-Exportprozess vertraut machen, bevor Sie die Schritte in diesem Handbuch durchführen. Weitere Informationen finden Sie unter Exportieren von Snapshots nach Amazon EC2.

Voraussetzungen

Exportieren Sie einen Lightsail-Blockspeicherdatenträger-Snapshot nach Amazon EC2. Weitere Informationen finden Sie unter Exportieren von Snapshots nach Amazon EC2.

Erstellen eines EBS-Volumes aus einem exportierten Lightsail-Blockspeicherdatenträger-Snapshot

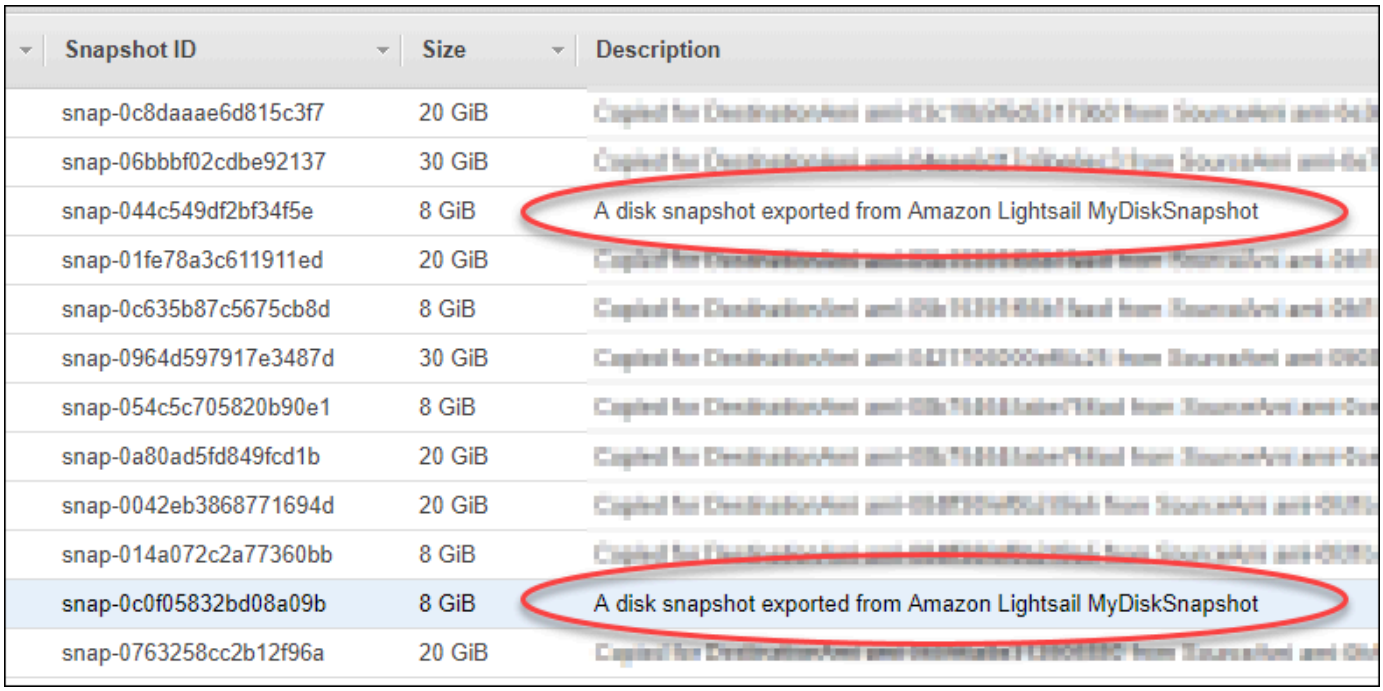
Verwenden Sie die Amazon-EC2-Konsole, um ein neues EBS-Volumen aus einem exportierten Lightsail-Blockspeicherdatenträger-Snapshot zu erstellen.

> **Note**
>
> Diese Schritte finden Sie auch in der Amazon-EC2-Dokumentation. Weitere Informationen finden Sie unter Wiederherstellen eines Amazon EBS-Volumes aus einem Snapshot in der Amazon EC2-Dokumentation.

So erstellen Sie ein EBS-Volumen aus einem exportierten Lightsail-Blockspeicherdatenträger-Snapshot

1. Melden Sie sich bei der Amazon-EC2-Konsole an.
2. Wählen Sie auf der Navigationsleiste die Region aus, in der sich Ihr Snapshot befindet.
3. Wählen Sie im Navigationsbereich Elastic Block Store und die Option Snapshots aus.
4. Suchen Sie den Snapshot des exportierten Lightsail-Blockspeicherdatenträgers und wählen Sie ihn aus.

   Der exportierte Datenträger-Snapshot kann, wie im folgenden Screenshot dargestellt, durch die Beschreibung Ein Datenträger-Snapshot aus Amazon Lightsail des EBS-Snapshots ermittelt werden:



5. Wählen Sie Actions (Aktionen) aus und klicken Sie auf Create Volume (Volumen erstellen).

6. Wählen Sie einen Volumentyp aus dem Dropdown-Menü Volume Type (Volumentyp) aus. Weitere Informationen finden Sie unter Amazon EBS-Volume-Typen in der Amazon EC2-Dokumentation.
7. Geben Sie unter Size (GiB) die Größe des Volumes ein oder stellen Sie sicher, dass die Standardgröße des Snapshots geeignet ist.
8. Geben Sie für bereitgestellte IOPS-SSD-Volumes für IOPS die maximale Anzahl der Ein-/Ausgabeoperationen pro Sekunde (input/output operations per second, IOPS) ein, die das Volume unterstützen sollte.
9. Wählen Sie unter Availability Zone die Availability Zone aus, in der das Volume erstellt werden soll. EBS-Volumes können nur EC2-Instances innerhalb derselben Availability Zone zugeordnet werden.
10. (Optional) Wählen Sie Create additional Tags, um dem Volume Tags (Markierungen) hinzuzufügen. Geben Sie für jeden Tag (Markierung) einen Tag (Markierung)-Schlüssel und einen Tag (Markierung)-Wert an.
11. Wählen Sie Create Volume. Nachdem Ihr Volumen erstellt wurde, wird es im Abschnitt Elastic Block Store > Volumen der Amazon-EC2-Konsole aufgelistet.

Nächste Schritte

Hier sind ein paar zusätzliche Schritte, die Sie nach dem Erstellen einer neuen Amazon-EC2-Instance durchführen können:

- Nachdem Sie ein Volume aus einem Snapshot wiederhergestellt haben, können Sie es an eine Instance anfügen und verwenden. Weitere Informationen finden Sie unter Anfügen eines Amazon-EBS-Volumes an eine Instance in der Amazon-EC2-Dokumentation.
- Wenn einen Snapshot auf einem Volume wiederherstellt haben, das größer als der Standard für den Snapshot ist, müssen Sie das Dateisystem auf dem Volume erweitern, um den zusätzlichen Speicherplatz nutzen zu können. Weitere Informationen finden Sie unter Ändern der Größe, IOPS oder des Typs eines EBS-Volumes unter Linux in der Amazon-EC2-Dokumentation.

Erstellen von Amazon-EC2-Instances aus exportierten Lightsail-Snapshots

Nachdem ein Lightsail-Instance-Snapshot exportiert wurde und in Amazon EC2 verfügbar ist (als AMI und als EBS-Snapshot), können Sie eine Amazon-EC2-Instance aus dem Snapshot erstellen, indem Sie die Seite Erstellen einer Amazon EC2-Instance in der Amazon Lightsail-Konsole verwenden,

die auch als „Assistent für das Upgrade auf Amazon EC2“ bekannt ist. Sie führt Sie durch die Konfigurationsoptionen der EC2-Instance, wie z. B. die Auswahl eines EC2-Instance-Typs, der Ihren Anforderungen entspricht, die Konfiguration Ihrer Sicherheitsgruppenports, das Hinzufügen eines Startskripts und vieles mehr. Der Assistent in der Lightsail-Konsole vereinfacht das Erstellen neuer EC2-Instances und der damit verbundenen Ressourcen.

> **Note**
>
> Um Amazon Elastic Block Store (Amazon EBS)-Volumes aus exportierten Blockspeicherdatenträger-Snapshots zu erstellen, lesen Sie Erstellen von Amazon-EBS-Volumes aus exportierten Datenträger-Snapshots.

Sie können neue EC2-Instances außerdem über die Lightsail-API, AWS CLI oder SDKs erstellen. Weitere Informationen finden Sie im CreateCloudFormationStack-Vorgang in der Lightsail-API-Dokumentation oder im create-cloud-formation-stack-Befehl in der AWS CLI-Dokumentation. Wenn Sie mit Amazon EC2 vertraut sind, können Sie die EC2-Konsole, die Amazon-EC2-API, AWS CLI oder SDKs verwenden. Weitere Informationen finden Sie unter Starten einer Instance mit dem Startassistenten für Instances oder Wiederherstellen eines Amazon-EBS-Volumes aus einem Snapshot in der Amazon-EC2-Dokumentation.

> **Important**
>
> Wir empfehlen, dass Sie sich mit dem Lightsail-Exportprozess vertraut machen, bevor Sie die Schritte in diesem Handbuch durchführen. Weitere Informationen finden Sie unter Exportieren von Snapshots nach Amazon EC2.

Inhalt

AWS CloudFormation-Stapel für Lightsail

Lightsail verwendet einen AWS CloudFormation-Stack, um EC2-Instances und die damit verbundenen Ressourcen zu erstellen. Weitere Informationen zu den CloudFormation-Stacks für Lightsail finden Sie unter AWS CloudFormation-Stacks für Lightsail.

Die folgenden zusätzlichen Berechtigungen müssen möglicherweise in IAM konfiguriert werden, je nachdem, welcher Benutzer die EC2-Instance über die Seite Eine Amazon-EC2-Instance erstellen erstellt:

- Wenn der Amazon-Konto-Stammbenutzer die EC2-Instance erstellt, fahren Sie mit dem Abschnitt Voraussetzungen in diesem Handbuch fort. Der Stammbenutzer verfügt bereits über die erforderlichen Berechtigungen, um EC2-Instances mit Lightsail zu erstellen.
- Wenn ein IAM-Benutzer die EC2-Instance erstellen soll, muss ein AWS-Kontoadministrator dem Benutzer die folgenden Berechtigungen hinzufügen. Weitere Informationen zum Ändern von Berechtigungen für einen Benutzer finden Sie unter Ändern von Berechtigungen für einen IAM-Benutzer in der IAM-Dokumentation.
  - Die folgenden Berechtigungen sind erforderlich, damit Benutzer Amazon-EC2-Instances mit Lightsail erstellen können:

    > **Note**
    >
    > Diese Berechtigungen ermöglichen die Erstellung des CloudFormation-Stacks. Wenn die Erstellung jedoch fehlschlägt, benötigt der Rollback-Prozess möglicherweise mehr Berechtigungen. Fehlende Berechtigungen können dazu führen, dass verbleibende Ressourcen in Amazon EC2 nicht zurückgesetzt werden. In diesem Fall können Sie zur AWS CloudFormation-Konsole wechseln und die EC2-Ressourcen manuell löschen. Weitere Informationen finden Sie unter AWS CloudFormation-Stacks für Lightsail.

    - ec2:DescribeAvailabilityZones
    - ec2:DescribeSubnets
    - ec2:DescribeRouteTables
    - ec2:DescribeInternetGateways
    - ec2:DescribeVpcs
    - cloudformation:CreateStack

    - cloudformation:ValidateTemplate
    - iam:CreateServiceLinkedRole
    - iam:PutRolePolicy
- Die folgenden Berechtigungen sind erforderlich, wenn der Benutzer Ports in der Sicherheitsgruppe für die EC2-Instance konfigurieren soll:
    - ec2:DescribeSecurityGroups
    - ec2:CreateSecurityGroup
    - ec2:AuthorizeSecurityGroupIngress
- Die folgenden Berechtigungen sind erforderlich, wenn der Benutzer eine Windows Server-Instance in Amazon EC2 erstellt:
    - ec2:DescribeKeyPairs
    - ec2:ImportKeyPair
- Die folgenden Berechtigungen sind erforderlich, wenn der Benutzer zum ersten Mal Amazon-EC2-Instances erstellt oder wenn die Virtual Private Cloud (VPC) nicht vollständig konfiguriert ist:
    - ec2:AssociateRouteTable
    - ec2:AttachInternetGateway
    - ec2:CreateInternetGateway
    - ec2:CreateRoute
    - ec2:CreateRouteTable
    - ec2:CreateSubnet
    - ec2:CreateVpc
    - ec2:ModifySubnetAttribute
    - ec2:ModifyVpcAttribute

Voraussetzungen

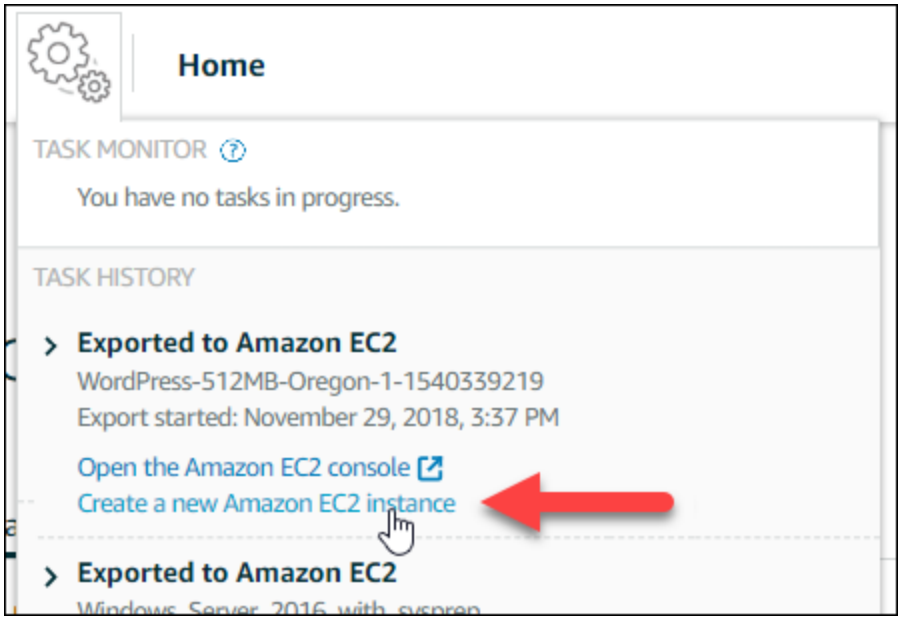
Einen Lightsail-Instance-Snapshot nach Amazon EC2 exportieren. Weitere Informationen finden Sie unter Exportieren von Snapshots nach Amazon EC2.

Aufrufen der Seite „Eine Amazon-EC2-Instance erstellen“ in der Lightsail-Konsole

Die Seite Eine Amazon-EC2-Instance erstellen in der Lightsail-Konsole kann nur von der Aufgabenüberwachung aus aufgerufen werden, nachdem ein Instance-Snapshot erfolgreich nach EC2 exportiert wurde.

Aufrufen der Seite „Eine Amazon-EC2-Instance erstellen“ in der Lightsail-Konsole

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie im oberen Navigationsbereich das Symbol Task monitor (Aufgabenüberwachung).
3. Suchen Sie den abgeschlossenen Instance-Snapshot-Export im Abschnitt Aufgabenverlauf und wählen Sie dann Eine neue Amazon-EC2-Instance erstellen aus.



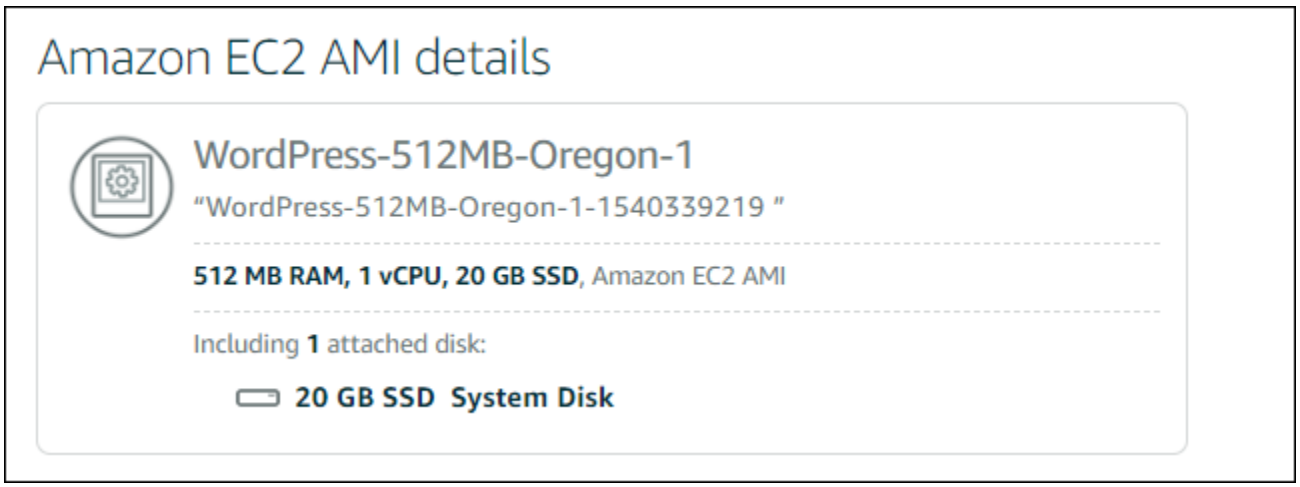
Die Seite Amazon-EC2-Instance erstellen wird angezeigt. Fahren Sie mit dem folgenden Abschnitt Erstellen einer Amazon-EC2-Instance in diesem Handbuch fort, um zu erfahren, wie Sie eine EC2-Instance über diese Seite konfigurieren und erstellen.

Erstellen einer Amazon-EC2-Instance

Verwenden Sie die Seite Eine Amazon-EC2-Instance erstellen, um eine EC2-Instance zu erstellen. Um mehr als eine EC2-Instance aus einem exportierten Lightsail-Snapshot zu erstellen, wiederholen Sie die folgenden Schritte mehrmals. Warten Sie aber, bis jede Instance erstellt ist, bevor Sie die nächste erstellen.

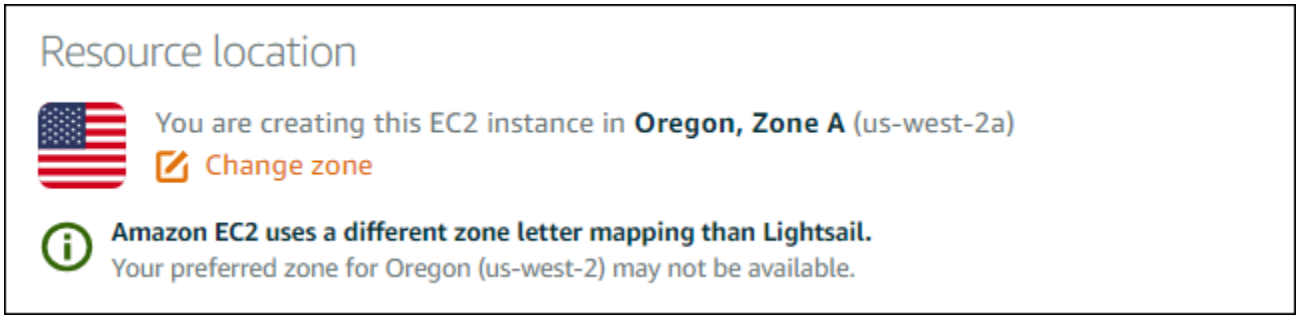
Erstellen einer Amazon-EC2-Instance

1. Vergewissern Sie sich im Abschnitt Amazon-EC2-AMI-Details auf der Seite, dass die angezeigten Details des Amazon Machine Image (AMI) mit den Spezifikationen der Quell-Lightsail-Instance übereinstimmen.

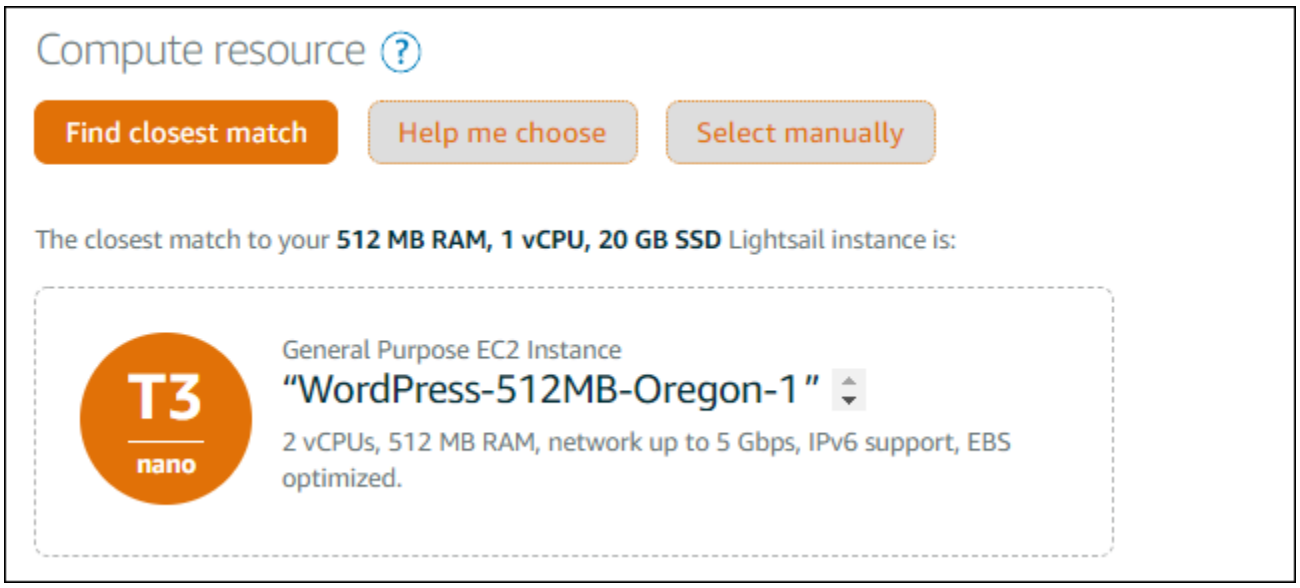


2. Ändern Sie im Abschnitt Resource location (Ressourcenstandort) auf der Seite bei Bedarf die Availability Zone Ihrer Instance. Die Amazon-EC2-Ressourcen werden in der gleichen AWS-Region erstellt wie der Quell-Lightsail-Snapshot.

> **Note**
>
> Nicht alle Availability Zones sind möglicherweise für alle Benutzer verfügbar. Die Auswahl einer nicht verfügbaren Availability Zone führt zu einem Fehler beim Erstellen der EC2-Instance.



3. Wählen Sie im Abschnitt Compute resource (Datenverarbeitungsressource) auf der Seite eine der folgenden Optionen:



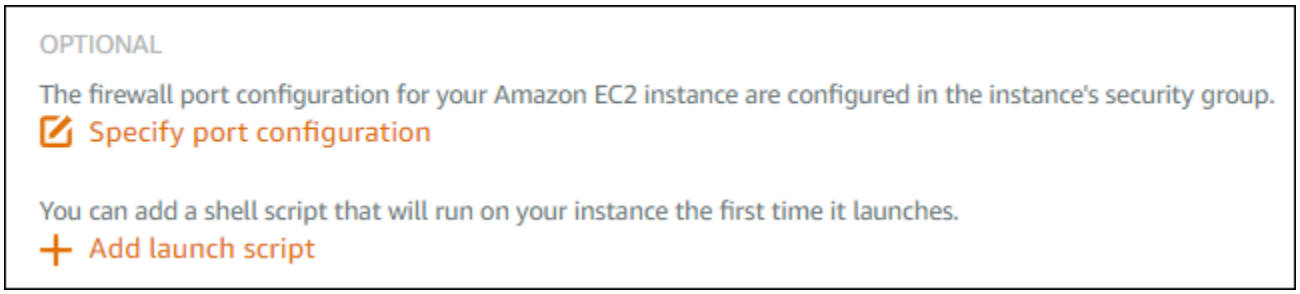
a. Beste Übereinstimmung suchen, um automatisch einen Amazon-EC2-Instance-Typ auszuwählen, der den Spezifikationen der Quell-Lightsail-Instance nahe kommt.

b. Hilfe bei der Auswahl, um einen kurzen Fragebogen über die Spezifikationen deiner neuen Amazon-EC2-Instance zu beantworten. Sie können aus Instance-Typen auswählen, die für die Datenverarbeitung oder den Arbeitsspeicher optimiert oder ausgewogen sind.

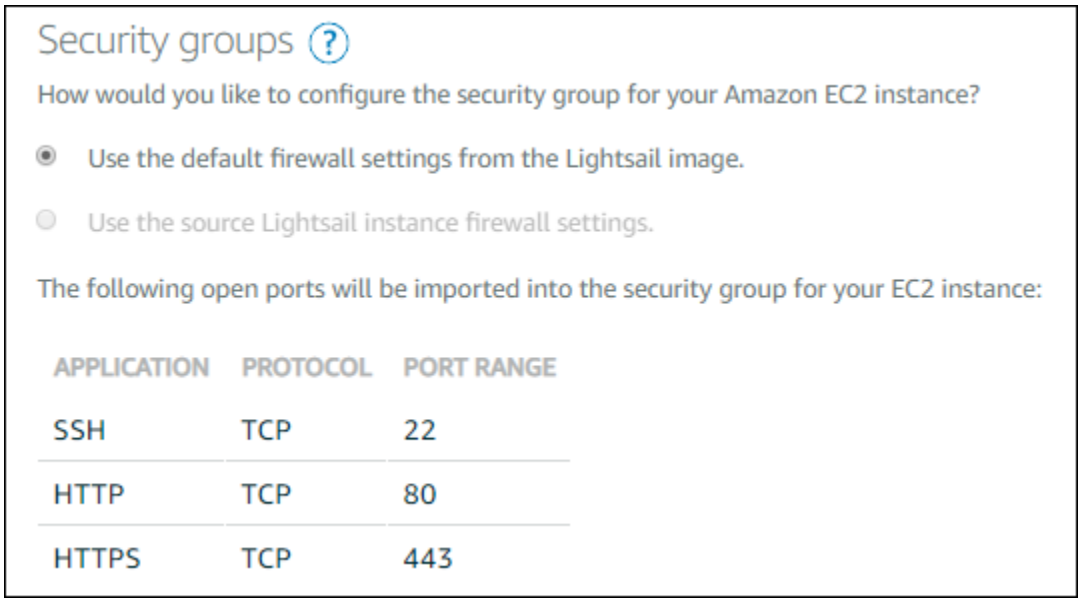
c. Manuell auswählen, um eine Liste der über die Seite Erstellen einer Amazon-EC2-Instance verfügbaren Instance-Typen anzuzeigen.

> **Note**
>
> Einige Lightsail-Instances sind mit den EC2-Instance-Typ der aktuellen Generation (T3, M5, C5 oder R5) nicht kompatibel, da sie für das erweiterte Netzwerk nicht aktiviert sind. Wenn Ihre Quell-Lightsail-Instance inkompatibel ist, müssen Sie beim Erstellen einer EC2-Instance aus Ihrem exportierten Snapshot einen Instance-Typ der vorherigen Generation (T2, M4, C4 oder R4) auswählen. Diese Instance-Typ-Optionen werden Ihnen auf der Seite Erstellen einer Amazon-EC2-Instance in der Lightsail-Konsole dargestellt.
>
> Um die EC2-Instance-Typen der neuesten Generation zu verwenden, wenn die Quell-Instance Lightsail inkompatibel ist, müssen Sie die neue EC2-Instance mit einem Instance-Typ der vorherigen Generation (T2, M4, C4 oder R4) erstellen, den Netzwerktreiber aktualisieren und die Instance dann auf den gewünschten Instance-Typ der aktuellen Generation aktualisieren. Weitere Informationen finden Sie unter Amazon-EC2-Instances für erweitertes Netzwerk.

4. Im Abschnitt Optional der Seite:



   a. Wählen Sie Portkonfiguration angeben aus, um die Firewall-Einstellungen für Ihre Amazon-EC2-Instance auszuwählen, und wählen Sie dann eine der folgenden Optionen aus:



      i. Use the default firewall settings from the Lightsail image (Verwenden der Standard-Firewall-Einstellungen aus dem &lightsail;-Image, um die Standard-Ports aus dem Quell-Lightsail-Blueprint auf Ihrer neuen EC2-Instance zu konfigurieren. Weitere Informationen zu den Standardports für Lightsail-Vorlagen finden Sie unter Firewall und Ports.

      ii. Use the source Lightsail instance firewall settings (Verwenden der Firewall-Einstellungen der Quell-&lightsail;-Instance, um die Ports der Quell-Lightsail-Instance auf Ihrer neuen EC2-Instance zu konfigurieren. Diese Option ist nur verfügbar, wenn die Quell-Lightsail-Instance noch aktiv ist.

   b. Wählen Sie im Abschnitt Launch script (Startskript) auf der Seite Add launch script (Launch-Script hinzufügen), wenn Sie ein Skript hinzufügen möchten, das Ihre EC2-Instance beim Start konfiguriert.

5. Bestimmen Sie im Abschnitt Connection security (Verbindungssicherheit) auf der Seite, wie Sie sich mit der Quell-Lightsail-Instance verbunden haben. Dadurch wird sichergestellt, dass Sie den richtigen SSH-Schlüssel erhalten, um sich mit Ihrer neuen EC2-Instance zu verbinden. Sie können sich mit einer der folgenden Methoden mit der Quell-Lightsail-Instance verbinden:

   a. Verwenden Sie das Standard-Lightsail-Schlüsselpaar für die Region der Quell-Instance – Laden Sie den eindeutigen Standard-Lightsail-Schlüssel für diese AWS-Region herunter und verwenden Sie ihn, um sich mit Ihrer EC2-Instance zu verbinden.

   > **Note**
   >
   > Das Standard-Lightsail-Schlüsselpaar wird bei Windows Server-Instances unter Lightsail immer verwendet.

   b. Mit Ihrem eigenen Schlüsselpaar – Suchen Sie den privaten Schlüssel und verbinden Sie sich mit ihm mit Ihrer EC2-Instance.

   > **Note**
   >
   > Lightsail speichert Ihren persönlichen privaten Schlüssel nicht. Daher ist die Möglichkeit, Ihren privaten Schlüssel herunterzuladen, nicht vorgesehen. Wenn Sie Ihren privaten Schlüssel nicht finden können, können Sie sich nicht mit Ihrer EC2-Instance verbinden.

6. Prüfen Sie im Abschnitt Storage resources (Speicherressourcen) der Seite, ob die zu erstellenden EBS-Volumes mit dem Systemdatenträger und allen angeschlossenen Blockspeicherdatenträgern für die Quell-Lightsail-Instance übereinstimmen.

7. Lesen Sie die wichtigen Details zur Erstellung von Ressourcen außerhalb von Lightsail.
8. Wenn Sie damit einverstanden sind, die Instance in Amazon EC2 zu erstellen, wählen Sie Ressourcen in EC2 erstellen aus.

   Lightsail bestätigt, dass Ihre Instance erstellt wird, und Informationen zum AWS CloudFormation-Stack werden angezeigt. Lightsail verwendet einen CloudFormation-Stack, um die Amazon-EC2-Instance und die damit verbundenen Ressourcen zu erstellen. Weitere Informationen finden Sie unter AWS CloudFormation-Stacks für Lightsail.

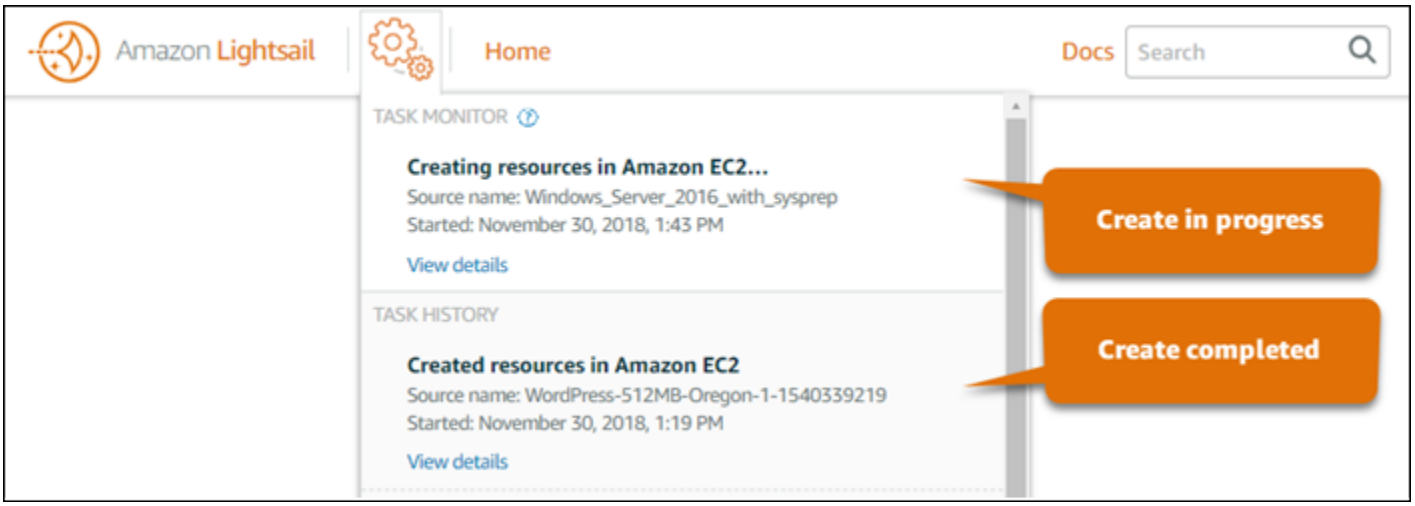
   Fahren Sie mit dem Abschnitt Verfolgen des Status Ihrer neuen Amazon-EC2-Instance in diesem Handbuch fort, um den Status Ihrer neuen EC2-Instance zu verfolgen.

   > **Important**
   >
   > Warten Sie, bis Ihre neue EC2-Instance erstellt wurde, um eine weitere EC2-Instance aus demselben exportierten Snapshot zu erstellen.

Verfolgen des Status Ihrer neuen Amazon-EC2-Instance

Verwenden Sie die Aufgabenüberwachung in der Lightsail-Konsole, um den Status Ihrer neuen EC2-Instance zu verfolgen. Er ist über den oberen Navigationsbereich auf allen Seiten der Lightsail-Konsole zugänglich. Weitere Informationen finden Sie unter Aufgabenüberwachung.

Die folgenden Informationen werden in der Aufgabenüberwachung für zu erstellende EC2-Instances angezeigt:



- Source name (Quellenname) – Der Name des Quell-Lightsail-Snapshots.
- Started (Gestartet) – Das Datum und die Uhrzeit, zu der der Erstellungsauftrag gestartet wurde.

Die folgenden Informationen werden in der Aufgabenüberwachung für erstellte EC2-Instances angezeigt:

- Created (Erstellt) wird angezeigt, wenn die Amazon EC2-Ressourcen erfolgreich erstellt wurden. Fahren Sie mit dem Abschnitt Nächste Schritte dieses Handbuchs fort, nachdem Ihre neue EC2-Instance bereit ist.
- Failed (Fehlgeschlagen) wird angezeigt, wenn es ein Problem bei der Erstellung der EC2-Instance gab.

Nächste Schritte

Hier sind ein paar zusätzliche Schritte, die Sie nach dem Erstellen einer Amazon-EC2-Instance durchführen können:

- Sie können sich mit Amazon-EC2-Instances so verbinden, wie Sie sich mit Lightsail-Instances verbinden. Das bedeutet, dass SSH für Linux- und Unix-Instances und RDP für Windows-Server-Instances verwendet werden. Der Browser-basierte SSH/RDP-Client, den Sie möglicherweise in der Lightsail-Konsole verwendet haben, ist jedoch je nach verwendeter Browserversion möglicherweise nicht in Amazon EC2 verfügbar, sodass Sie möglicherweise Ihren eigenen SSH/RDP-Client konfigurieren müssen, um eine Verbindung zu Ihren EC2-Instances herzustellen. Weitere Informationen finden Sie in den folgenden Anleitungen:
  - Verbinden mit einer Amazon-EC2-Linux- oder Unix-Instance, die aus einem Lightsail-Snapshot erstellt wurde
  - Verbinden mit einer Instance von Amazon EC2 Windows Server, die aus einem Lightsail-Snapshot erstellt wurde
- Linux- oder Unix-Instances in Amazon EC2, die aus Lightsail-Snapshots erstellt wurden, können dauerhaft gespeicherte SSH-Schlüssel von Lightsail enthalten. Wir empfehlen, diese Schlüssel zu entfernen, um Ihre EC2-Instance besser zu sichern. Weitere Informationen finden Sie unter Sichern einer Amazon-EC2-Linux- oder Unix-Instance, die aus einem Lightsail-Snapshot erstellt wurde.

Nachdem Ihre EC2-Instance erstellt wurde, müssen Sie möglicherweise noch einige weitere Schritte durchführen, damit sie wie die Quell-Lightsail-Instance konfiguriert ist. Hier sind ein paar zusätzliche Schritte zur Konfiguration Ihrer EC2-Instance:

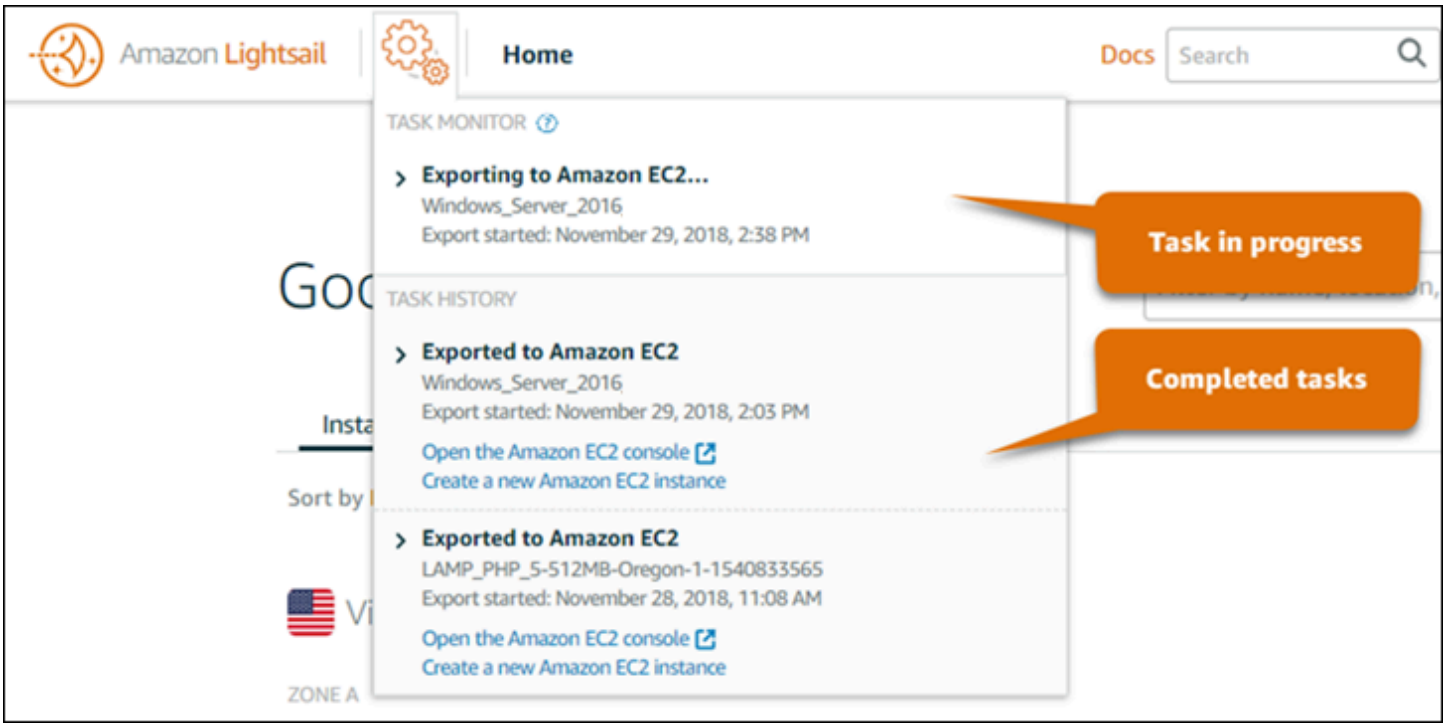
- Konfigurieren Sie die Firewall-Einstellungen, indem Sie die Sicherheitsgruppe für Ihre Amazon-EC2-Instance bearbeiten. Weitere Informationen finden Sie unter Amazon-EC2-Sicherheitsgruppen für Linux-Instances oder Amazon-EC2-Sicherheitsgruppen für Windows-Instances in der Amazon-EC2-Dokumentation.
- Wenn Sie eine statische Lightsail-IP erstellt und an Ihre Lightsail-Instance angehängt haben, dann sollten Sie eine elastische IP erstellen und an Ihre Amazon-EC2-Instance anhängen. Weitere Informationen finden Sie unter Elastische IP-Adressen in der Amazon-EC2-Dokumentation.
- Wenn Sie eine Lightsail-DNS-Zone erstellt und eine Domain für Ihre Lightsail-Instance konfiguriert haben, dann sollten Sie eine Amazon-Route-53-DNS-Zone erstellen, diese verwenden, um die DNS Ihrer Domain zu verwalten und Ihre Domain auf Ihre neue Amazon-EC2-Instance leiten. Weitere Informationen finden Sie unter Konfigurieren von Amazon Route 53 als Ihr DNS-Service und Amazon Route 53 zum DNS-Service für eine bestehende Domain machen in der Amazon-Route-53-Dokumentation.
- Wenn Sie einen Lightsail-Load-Balancer erstellt und für Ihre Lightsail-Instances konfiguriert haben, dann sollten Sie einen Application Load Balancer für Ihre Amazon-EC2-Instances konfigurieren.

Weitere Informationen finden Sie unter Erste Schritte mit Application Load Balancern in der Elastic-Load-Balancing-Dokumentation.

- Lightsail-Datenbanken können von Amazon-EC2-Instances nicht aufgerufen werden. Wenn die Lightsail-Instance, die Sie nach Amazon EC2 exportiert haben, mit einer Lightsail-Datenbank verbunden ist, müssen Sie diese Datenbank manuell nach Amazon Relational Database Service (Amazon RDS) migrieren, um von der neuen Amazon-EC2-Instance auf ihre Daten zuzugreifen. Weitere Informationen finden Sie unter Importieren von Daten in eine Amazon-RDS-MySQL- oder -MariaDB-Datenbank-Instance mit reduzierter Ausfallzeit und Verbinden mit einer Amazon-RDS-DB-Instance.

Lightsail-Konsole-Aufgabenüberwachung

Die Aufgabenüberwachung in der Amazon Lightsail-Konsole verfolgt den Status des Exports von Lightsail-Snapshots nach Amazon EC2 oder der Erstellung neuer EC2-Instances aus exportierten Instance-Snapshots. Diese Aufgaben können je nach Größe und Konfiguration der Quell-Instance oder des Quell-Blockspeichers eine Weile in Anspruch nehmen. Der Aufgabenmonitor zeigt die letzten 20 Aufgaben an, die gerade ausgeführt werden oder abgeschlossen wurden. Er ist über den oberen Navigationsbereich auf allen Seiten der Lightsail-Konsole zugänglich. Das Aufgabenmonitorsymbol ist orange, wenn eine Aufgabe ausgeführt wird, oder grau, wenn alle Aufgaben abgeschlossen sind.



Weitere Informationen zum Exportieren von Lightsail-Snapshots nach Amazon EC2 oder zum Erstellen von EC2-Instances aus exportierten Snapshots finden Sie in den folgenden Handbüchern:

- Exportieren von Snapshots nach Amazon EC2
- Erstellen von Amazon-EC2-Instances aus exportierten Snapshots

Domänenregistrierung in Amazon Lightsail

Ihre Website benötigt einen Namen, wie zum Beispiel `example.com`. Mit Amazon Lightsail können Sie einen Namen für Ihre Website oder Webanwendung registrieren, bekannt als Domainname. Um auf Ihre Website zuzugreifen, geben Benutzer Ihren Domänennamen in ihren Webbrowser ein.

Verwenden Sie den Tab Domains und DNS in der Amazon Lightsail-Konsole, um Domainnamen zu registrieren und zu verwalten. Lightsail nutzt Amazon Route 53, einen hochverfügbaren und skalierbaren Domain Name System (DNS)-Webservice, um Domains für Sie zu registrieren. Nachdem Ihre Domäne registriert ist, können Sie sie Ihren Lightsail-Ressourcen zuweisen oder DNS-Datensätze für sie verwalten. Allgemeine Informationen über DNS finden Sie unter DNS.

Weitere Informationen zur Domänenregistrierung in Amazon Lightsail finden Sie, wenn Sie weiterlesen.

Inhalt

Funktionsweise der Domainregistrierung

Die nachstehende Übersicht veranschaulicht, wie Sie einen Domänennamen in Amazon Lightsail registrieren:

1. Vergewissern Sie sich, dass der gewünschte Domänenname für die Verwendung im Internet verfügbar ist. Wenn der gewünschte Domänenname nicht verfügbar ist, können Sie einen anderen Namen ausprobieren oder nur die Top-Level-Domäne wie .com in eine andere Top-Level-Domäne wie z. B. .org oder .net ändern. Eine Liste der von Lightsail unterstützten Top-Level-Domains (TLDs) finden Sie unter Domains, die Sie mit Amazon Lightsail registrieren können.
2. Registrieren Sie den Domänennamen mit Lightsail. Wenn Sie eine Domäne registrieren, geben Sie Namen Kontaktinformationen für den Domäneneigentümer und andere Kontakte an.

Nach dem Registrierungsprozess senden wir die von Ihnen bereitgestellten Informationen an die Vergabestelle für die Domäne. Die Vergabestelle ist ein Unternehmen, das von ICANN (Internet

Corporation for Assigned Names and Numbers) für die Verarbeitung von Domänenregistrierungen für bestimmte Top-Level-Domänen (TLDs) zugelassen wurde. Die Vergabestelle für die Domäne ist entweder Amazon Registrar oder unsere Partner-Vergabestelle, Gandi.

Amazon Registrar und Gandi blenden standardmäßig unterschiedliche Informationen aus: Amazon Registrar, Inc. blendet alle Ihre Kontaktinformationen aus und Gandi blendet alle Ihre Kontaktinformationen außer dem Namen der Organisation aus.

- Unter Domains, die Sie mit Amazon Lightsail registrieren können können Sie ermitteln, wer die Vergabestelle für die Domain ist.
- Die Vergabestelle sendet Ihre Informationen zur Registrierungsstelle für die Domäne. Eine Registrierungsstelle ist ein Unternehmen, das Domänenregistrierungen für eine oder mehrere Domänen oberster Ebene (Top-Level-Domänen), wie z. B. .com, verkauft.
- Die Registrierungsstelle speichert die Informationen über Ihre Domäne in ihrer eigenen Datenbank und speichert auch einige Informationen in der öffentlichen WHOIS-Datenbank.

Weitere Informationen zum Registrieren eines Domainnamens finden Sie unter Registrieren einer neuen Domain.

Nachdem Sie eine Domain mit Lightsail registriert haben, wird Route 53 automatisch zum DNS-Service für Ihre Domain, indem Ihrer Domain eine Reihe von Namenservern zugewiesen wird. Ein Namenserver ist ein Server, der hilft, Domänennamen in IP-Adressen umzuwandeln.

In Lightsail werden automatisch die folgenden Schritte ausgeführt, um selbst zum DNS-Service für die Domäne zu werden:

- Erstellt eine Lightsail-DNS-Zone, die denselben Namen hat wie die Domäne.
- Weist eine Gruppe von vier Namenservern zur Lightsail-DNS-Zone zu.
- Ersetzt die Route-53-Namenserver der Domain durch die Namenserver aus Ihrer Lightsail-DNS-Zone.

Wenn Sie bereits einen Domainnamen bei einer anderen Vergabestelle registriert haben, können Sie die DNS-Verwaltung der Domain an Lightsail übertragen. Dies ist nicht erforderlich, um andere Lightsail-Funktionen zu nutzen. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.

Domänen, die Sie in Lightsail registrieren können

Lightsail verwendet dieselben generischen Top-Level-Domains (TLDs) wie Route 53. Eine Liste generischer TLDs, mit denen Sie Domains in Lightsail registrieren können, finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können im Entwicklerhandbuch für Amazon Route 53.

Wenn die TLD nicht in der Liste enthalten ist oder Sie eine geografische Domain registrieren möchten, empfehlen wir Ihnen, die Route-53-Konsole zu verwenden. Ihre geografische Domain ist in der Lightsail-Konsole verfügbar, nachdem sie mit Route 53 registriert wurde. Weitere Informationen finden Sie unter Geografische Top-Level-Domains im Entwicklerhandbuch für Amazon Route 53.

Preise für die Domainregistrierung

Lightsail verwendet Route 53 für die Domainregistrierung. Daher gilt die Route-53-Preisgestaltung auch für Lightsail-Registrierungen.

Informationen zu den Kosten für die Registrierung von Domains finden Sie unter Domains, die Sie in Amazon Route 53 registrieren können im Entwicklerhandbuch für Amazon Route 53.

Weitere Informationen zu Domänen

Die folgenden Artikel können Ihnen bei der Verwaltung Ihrer Domänen in Lightsail helfen:

- DNS
- Format von Domainnamen
- Eine Lightsail-Domain in Amazon Route 53 verwalten
- Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain
- Erneuerung der Domainregistrierung
- Bearbeiten oder Löschen einer DNS-Zone
- Verweisen Ihrer Domain auf einen Load Balancer
- Verweisen Sie Ihre Domain auf eine Verteilung
- Verweisen Ihrer Domain auf eine Instance
- Weiterleiten von Datenverkehr für Ihre Domain zu einem Container-Service

DNS in Amazon Lightsail

Benutzer können auf die Webanwendung auf Ihrer Lightsail-Instance zugreifen, indem sie zur öffentlichen Internetprotokolladresse (IP) Ihrer Instance navigieren, bei der es sich um eine IPv4- oder IP6-Adresse handeln kann. Allerdings sind IP-Adressen oft komplex und für Menschen schwer zu merken. Daher sollten Benutzer nach einem easy-to-remember Domainnamen suchen lassen, um beispielsweise `example.com` auf die Webanwendung auf Ihrer Instance zuzugreifen. Dies wird durch das Domain Name System (DNS) erreicht, das als Verzeichnis fungiert, das registrierte Domainnamen auf IP-Adressen abbildet.

Um den Traffic für Ihren Domainnamen an Ihre Lightsail-Instance weiterzuleiten, fügen Sie einen Adresseintrag (A) hinzu, der Ihren Domainnamen auf die statische IPv4-Adresse Ihrer Instance verweist, oder einen AAAA-Eintrag, der auf die IPv6-Adresse Ihrer Instance verweist. Wenn Sie einen Domainnamen mit Lightsail registriert haben, können Sie die DNS-Einträge aus der DNS-Zone verwalten, die bei der Registrierung des Domainnamens erstellt wurde. Wenn Ihre Domain über einen anderen Registrar registriert wurde, können Sie die DNS-Einträge beim Registrar verwalten oder die Verwaltung des DNS Ihrer Domain an Lightsail übertragen.

Um die Zuordnung Ihres Domainnamens zu Ihrer Lightsail-Instance zu vereinfachen, empfehlen wir Ihnen, die Verwaltung der DNS-Einträge Ihrer Domain an Lightsail zu übertragen, indem Sie eine DNS-Zone erstellen. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain. Sie können in Lightsail bis zu sechs DNS-Zonen erstellen. Wenn Sie mehr als sechs DNS-Zonen benötigen, empfehlen wir Ihnen, die DNS aller Domains mit Route 53 zu verwalten. Sie können Route 53 verwenden, um Ihren Domainnamen auf Ihre Lightsail-Instanz zu verweisen. Weitere Informationen zum Verwalten von DNS mit Route 53 finden Sie unter Eine Domain mit Amazon Route 53 auf eine Instance verweisen.

DNS-Terminologie

Damit Sie DNS für Ihre Domäne verwalten können, gibt es einige Begriffe, mit denen Sie vertraut sein sollten.

Apex Domäne/Stamm-Domäne

> Eine Apex-Domäne, auch bekannt als Stammdomäne, ist eine Domäne, die nicht Teil einer Subdomäne ist. Ein Beispiel für eine Apex-Domäne ist `example.com`. Beispiele für Subdomänen sind dagegen `www.example.com` und `blog.example.com`. Dies sind Subdomänen, da sie die Teile einer Subdomäne `www` und `blog` enthalten.

Domain Name System (DNS)

DNS leitet easy-to-remember Domainnamen, z. B. `example.com`, an die IP-Adressen von Webservern weiter.

Weitere Informationen finden Sie unter Domain Name System in Wikipedia.

DNS-Datensatz

Ein DNS-Datensatz ist ein Zuweisungsparameter. Er teilt dem DNS-Server mit, mit welcher IP-Adresse oder welchem Hostnamen eine Domäne oder Subdomäne verbunden ist.

Weitere Informationen finden Sie unter Liste der DNS-Datensatztypen auf Wikipedia.

DNS-Zone

Eine DNS-Zone ist ein Container, der Informationen darüber enthält, wie Sie den Datenverkehr im Internet für eine bestimmte Domäne weiterleiten möchten, wie z. B. `example.com`, und seine Subdomänen, wie z. B. `blog.example.com`.

Weitere Informationen finden Sie unter DNS-Zone in Wikipedia.

Vergabestelle für Domänennamen

Eine Domänennamen-Vergabestelle, auch bekannt als Domänennamen-Provider, ist ein Unternehmen oder eine Organisation, die die Vergabe von Domänennamen verwaltet. Sie können eine Domain kaufen oder eine bestehende Domain mit Lightsail, Amazon Route 53 oder einem anderen Domainnamen-Registrar verwalten.

Weitere Informationen finden Sie unter Domain Name Registrar auf Wikipedia.

Namenserver

Ein Nameserver leitet Verkehr an Ihre Domäne weiter. In Lightsail ist der Nameserver eine AWS Instanz, die einen Netzwerkdienst ausführt, um easy-to-remember Domainnamen in IP-Adressen zu übersetzen. Lightsail bietet mehrere AWS Nameserver-Optionen (z. B. `ns-NN.awsdns-NN.com`), um den Traffic an Ihre Domain weiterzuleiten. Sie können aus diesen AWS Nameservern wählen, wenn Sie Ihre Domain über einen Domain-Registrar ändern.

Weitere Informationen finden Sie unter Nameserver in Wikipedia.

Unterdomain

Eine Unterdomäne ist alles in der Domänenhierarchie (mit Ausnahme der Root-Domäne), das Teil der größeren Domäne ist. Zum Beispiel ist `blog` der Subdomänenteil der `blog.example.com` Subdomäne.

Weitere Informationen finden Sie unter Subdomain in Wikipedia.

Time to Live (TTL)

TTL bestimmt die Lebensdauer eines DNS-Eintrags auf lokal auflösenden Nameservern. Eine kürzere Zeit bedeutet beispielsweise weniger Wartezeit, bis Änderungen in Kraft treten. TTL kann in der Lightsail-DNS-Zone nicht konfiguriert werden. Stattdessen verwenden alle Lightsail-DNS-Einträge standardmäßig eine TTL von 60 Sekunden.

Weitere Informationen finden Sie unter Time to Live in Wikipedia.

Wildcard-DNS-Datensatz

Ein Wildcard-DNS-Eintrag deckt Anforderungen für nicht vorhandene Domänennamen ab. Ein Wildcard-DNS-Eintrag wird angegeben, indem das Sternchensymbol (*) als äußerster linker Teil eines Domänennamens verwendet wird, wie z. B. `*.example.com` oder `*example.com`.

> **Note**
>
> Lightsail-DNS-Zonen unterstützen Platzhaltereinträge für Nameserverdomänen (`*awsdns.com`), die in einem Nameserver-Datensatz (NS) definiert sind.

In der Lightsail-DNS-Zone unterstützte DNS-Eintragstypen

(A) Adressen-Datensatz

Ein A-Datensatz ordnet eine Domäne, wie beispielsweise `example.com`, oder eine Subdomäne, wie `blog.example.com`, der IP-Adresse eines Webservers zu.

In der Lightsail-DNS-Zone möchten Sie beispielsweise den Web-Traffic für `example.com` (den Apex der Domain) zu Ihrer Instance weiterleiten. Sie würden einen A-Datensatz erstellen, ein @-Symbol in das Textfeld Subdomain (Subdomäne) und die IP-Adresse Ihres Webservers in das Textfeld Resolves to address (Zugewiesen zur Adresse) eingeben.

Weitere Informationen über den A-Datensatz finden Sie unter Liste der DNS-Datensatztypen auf Wikipedia.

AAAA-Datensätze

Ein AAAA-Datensatz ordnet eine Domäne, wie beispielsweise `example.com`, oder eine Subdomäne, wie `blog.example.com`, der IPv6-Adresse eines Webservers zu.

In der Lightsail-DNS-Zone möchten Sie beispielsweise den Web-Datenverkehr für `example.com` (den Scheitelpunkt der Domäne) auf Ihre Instance über das IPv6-Protokoll leiten. Sie würden einen AAAA-Datensatz erstellen, ein @-Symbol in das Textfeld Subdomain (Subdomäne) und die IP-Adresse Ihres Webservers in das Textfeld Resolves to address (Zugewiesen zur Adresse) eingeben.

Weitere Informationen zum AAAA-Datensatz finden Sie unter Domain Name System for IPv6 in Wikipedia aus.

> **Note**
>
> Lightsail unterstützt keine statischen IPv6-Adressen. Wenn Sie Ihre Lightsail-Ressource löschen und eine neue Ressource erstellen oder wenn Sie IPv6 auf derselben Ressource deaktivieren und erneut aktivieren, müssen Sie möglicherweise Ihren AAAA-Eintrag aktualisieren, sodass er die neueste IPv6-Adresse für die Ressource wiedergibt.

Kanonischer Name, CNAME-Datensatz

Ein CNAME-Datensatz ordnet einen Alias oder eine Unterdomäne, wie z. B. `blog.example.com`, einer anderen Domäne oder Subdomäne zu.

In der Lightsail-DNS-Zone möchten Sie beispielsweise den Webverkehr für `www.example.com` nach weiterleiten. `example.com` In diesem Fall würden Sie einen Alias-CNAME-Eintrag für `www` mit einer "resolves to"-Adresse von `example.com` erstellen.

Weitere Informationen finden Sie unter CNAME-Akte in Wikipedia.

Mail Exchanger, MX-Datensatz

Ein MX-Datensatz ordnet eine Subdomäne, wie beispielsweise `mail.example.com`, einer E-Mail-Adresse mit Werten für die Priorität zu, wenn mehrere Server definiert sind.

In der Lightsail-DNS-Zone möchten Sie beispielsweise E-Mails an den `10 inbound-smtp.us-west-2.amazonaws.com` WorkMail Amazon-Server `mail.example.com` weiterleiten. In diesem Fall erstellen Sie einen MX-Datensatz mit einer Subdomäne `example.com`, eine Priorität von `10` und eine "resolves to"-Adresse `inbound-smtp.us-west-2.amazonaws.com`.

Weitere Informationen finden Sie unter MX Record in Wikipedia.

Nameserver (NS)-Datensatz

Ein NS-Datensatz delegiert eine Subdomäne, wie `test.example.com`, an einen Nameserver, wie z. B. `ns-NN.awsdns-NN.com`.

Weitere Informationen finden Sie unter Nameserver in Wikipedia.

Service-Locator, SRV-Datensatz

Ein SRV-Datensatz ordnet eine Subdomain, wie beispielsweise `service.example.com`, einer Serviceadresse mit Werten für Priorität, Gewichtung und Portnummer zu. Telefonie oder Instant Messaging sind nur einige der Dienste, die typischerweise mit SRV-Datensätzen verbunden sind.

In der Lightsail-DNS-Zone möchten Sie beispielsweise den Verkehr für `service.example.com` nach weiterleiten. `1 10 5269 xmpp-server.example.com` Sie erstellen einen SRV-Datensatz mit der Priorität `1`, der Gewichtung `10`, einer Portnummer `5269` und einer "maps to"-Adresse `xmpp-server.example.com`.

Weitere Informationen finden Sie unter SRV Record in Wikipedia.

Text, TXT-Datensatz

Ein TXT-Datensatz bildet eine Subdomäne in Klartext ab. Sie erstellen TXT-Datensätze, um den Besitz Ihrer Domain für einen Dienstanbieter zu bestätigen.

In der Lightsail-DNS-Zone möchten Sie beispielsweise mit antworten, `23223a30-7f1d-4sx7-84fb-31bdes7csdbb` wenn der `_amazonchime.example.com` Hostname abgefragt wird. In diesem Fall würden Sie einen TXT-Eintrag mit einem Subdomänenwert von `_amazonchime` und einem "responds with" Wert von `23223a30-7f1d-4sx7-84fb-31bdes7csdbb` erstellen.

Weitere Informationen finden Sie unter TXT Record in Wikipedia.

Themen

- Erstellen einer Lightsail-DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain
- Bearbeiten oder Löschen einer DNS-Zone in Lightsail
- Wie Internetdatenverkehr in Lightsail an Ihre Website weitergeleitet wird
- Verweisen Ihrer Lightsail-Domain auf eine Instance
- Verweisen Ihrer Lightsail-Domain auf einen Load Balancer
- Aktualisieren Ihrer Lightsail-Domainnamenserver, um einen anderen DNS-Service zu verwenden

- Verwenden von Amazon Route 53, um eine Domain auf eine Lightsail Instance zu verweisen

Erstellen einer Lightsail-DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain

Um Datenverkehr für einen Domänennamen, z. B. `example.com`, an eine Amazon Lightsail-Instance weiterzuleiten, fügen Sie dem Domain Name System (DNS) Ihrer Domäne einen Datensatz hinzu. Sie können die DNS-Datensätze Ihrer Domain über die Vergabestelle verwalten, bei der Sie Ihre Domain registriert haben, oder Sie können sie mit Lightsail verwalten.

Wir empfehlen Ihnen, die Verwaltung der DNS-Datensätze Ihrer Domain auf Lightsail zu übertragen. Auf diese Weise können Sie Ihre Domain und Rechenressourcen effizient an einem Ort verwalten – Lightsail. Sie können die DNS-Datensätze Ihrer Domain mit Lightsail verwalten, indem Sie eine Lightsail-DNS-Zone erstellen. Sie können bis zu sechs Lightsail-DNS-Zonen erstellen. Wenn Sie mehr als sechs DNS-Zonen benötigen, da Sie mehr als sechs Domainnamen verwalten, empfehlen wir Ihnen, den DNS aller Domains mit Amazon Route 53 zu verwalten. Sie können Route 53 verwenden, um den Datenverkehr für Ihre Domain an Ihre Lightsail-Ressourcen weiterzuleiten. Weitere Informationen zum Verwalten von DNS mit Route 53 finden Sie unter Eine Domain mit Amazon Route 53 auf eine Instance verweisen.

Dieses Handbuch zeigt Ihnen, wie Sie eine Lightsail-DNS-Zone für Ihre Domäne erstellen und die Verwaltung der DNS-Datensätze Ihrer Domäne an Lightsail übertragen. Nachdem Sie die Verwaltung der DNS-Datensätze Ihrer Domain an Lightsail übertragen haben, verwalten Sie weiterhin Erneuerungen und Abrechnungen für Ihre Domain bei der Vergabestelle Ihrer Domain.

> **Important**
>
> Alle Änderungen, die Sie am DNS Ihrer Domain vornehmen, können mehrere Stunden dauern, damit sich die Verbreitung über das DNS im Internet ausbreiten. Aus diesem Grund sollten Sie die DNS-Datensätze Ihrer Domain beim aktuellen DNS-Hosting-Anbieter Ihrer Domain beibehalten, während die Übertragung der Verwaltung an Lightsail propagiert wird. Dadurch wird sichergestellt, dass der Datenverkehr für Ihre Domain während der Übertragung ununterbrochen zu Ihren Ressourcen weitergeleitet wird.

Inhalt

- Schritt 2: Erstellen einer DNS-Zone in der Lightsail-Konsole
- Schritt 3: Hinzufügen von Datensätzen zur DNS-Zone
- Schritt 4: Ändern des Nameservers beim aktuellen DNS-Hosting-Provider Ihrer Domain

Schritt 1: Erfüllen der Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies nicht ohnehin bereits der Fall ist:

1. Registrieren Sie einen Domainnamen Bestätigen Sie dann, dass Sie über Administratorzugriff verfügen, um die Namensserver der Domain zu bearbeiten.

   Wenn Sie einen registrierten Domänennamen benötigen, können Sie eine Domäne mit Lightsail registrieren. Weitere Informationen finden Sie unter Domainregistrierung.
2. Vergewissern Sie sich, dass die erforderlichen DNS-Datensatztypen für Ihre Domain von der Lightsail-DNS-Zone unterstützt werden. Die Lightsail-DNS-Zone unterstützt derzeit die Datensatztypen Adresse (A und AAAA), kanonischer Name (CNAME), Mail Exchanger (MX), Nameserver (NS), Service Locator (SRV) und Text (TXT). Für NS-Einträge können Sie Wildcard-DNS-Datensätze verwenden.

   Wenn die für Ihre Domäne erforderlichen DNS-Datensatztypen von der Lightsail-DNS-Zone nicht unterstützt werden, sollten Sie Route 53 als DNS-Hosting-Anbieter Ihrer Domäne verwenden, da es eine größere Anzahl von Datensatztypen unterstützt. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen und Amazon Route 53 als DNS-Service für eine bestehende Domain einrichten im Handbuch für Entwickler von Amazon Route 53.
3. Erstellen Sie eine Lightsail-Instance, auf die Sie Ihre Domain verweisen. Weitere Informationen finden Sie unter Erstellen einer Instance.
4. Erstellen Sie eine statische IP und fügen Sie sie an Ihre Lightsail-Instance an. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

Schritt 2: Erstellen einer DNS-Zone in der Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um eine DNS-Zone in Lightsail zu erstellen. Wenn Sie eine DNS-Zone erstellen, müssen Sie den Domainnamen angeben, für den die DNS-Zone gelten soll.

1. Melden Sie sich bei der Lightsail-Konsole an.

2. Wählen Sie die Registerkarte Domains & DNS (Domains und DNS) und dann Create DNS zone (DNS-Zone erstellen) aus.
3. Wählen Sie eine der folgenden Optionen:

   - Verwenden Sie eine bei Amazon Route 53 registrierte Domain, um eine Domain anzugeben, die bei Amazon Route 53 registriert wurde
   - Verwenden Sie eine Domain von einer anderen Vergabestelle, um eine Domain anzugeben, die bei einer anderen Vergabestelle registriert wurde.
4. Wählen Sie den Namen Ihrer registrierten Domains aus oder geben Sie ihn ein, z.`example.com` B.

   Es ist nicht notwendig, `www` bei der Eingabe Ihres Domainnamens anzugeben. Sie können das `www` mit einem (A) Adressen-Datensatz als Teil von Schritt 3: Hinzufügen von Datensätzen zur DNS-Zone später in dieser Anleitung hinzufügen.

   > **Note**
   >
   > Lightsail-DNS-Zonen werden in der Virginia (`us-east-1`) erstelltAWS-Region. Sie erhalten einen Ressourcennamen-Konfliktfehler („einige Namen werden bereits verwendet“), wenn Sie eine Ressource in dieser Region genauso benannt haben wie die Lightsail-DNS-Zone (), die `example.com`Sie erstellen möchten.
   > Um den Fehler aufzulösen, erstellen Sie einen Snapshot der Ressource. Erstellen Sie eine neue Ressource aus dem Snapshot und geben Sie ihr einen neuen, eindeutigen Namen. Löschen Sie dann die ursprüngliche Ressource, die den gleichen Namen wie die Domäne trägt, für die Sie eine Lightsail-DNS-Zone erstellen möchten.
5. Wählen Sie Create DNS zone (DNS-Zone erstellen).

   Sie werden zur Seite Assignments (Zuweisungen) der DNS-Zone weitergeleitet, auf der Sie die Zuweisungen von Domainressourcen verwalten können. Verwenden Sie Zuweisungen, um eine Domain auf Ihre Lightsail-Ressourcen wie Load Balancer und Instances zu verweisen.

Schritt 3: Hinzufügen von Datensätzen zur DNS-Zone

Führen Sie die folgenden Schritte aus, um Datensätze zur DNS-Zone Ihrer Domain hinzuzufügen. DNS-Datensätze geben an, wie der Internetverkehr für die Domain weitergeleitet wird. Beispielsweise können Sie den Datenverkehr für den Scheitelpunkt Ihrer Domain, wie z. B. `example.com`, an eine

Instance weiterleiten, und den Datenverkehr für eine Subdomain, wie z. B. `blog.example.com` an eine andere Instance leiten.

1. Wählen Sie auf der Seite mit den DNS-Zonenzuweisungen die Registerkarte DNS records (DNS-Datensätze) aus.

   Ihre DNS-Zonen sind auf der Registerkarte Domains und DNS der Lightsail-Konsole aufgeführt.

   > **Note**
   >
   > Auf der Seite DNS zone Assignments (DNS-Zonenzuweisungen) können Sie hinzufügen, entfernen oder ändern, auf welche Lightsail-Ressource Ihre Domain verweist. Sie können Domains auf Lightsail-Instances, Distributionen, Container-Services, Load Balancer, statische IP-Adressen und mehr verweisen. Auf der Seite DNS records (DNS-Datensätze) können Sie DNS-Datensätze Ihrer Domain hinzufügen, bearbeiten oder löschen.

2. Wählen Sie eine der folgenden Datensatztypen aus:

   (A) Adressen-Datensatz

   Ein Datensatz ordnet eine Domäne, z. B. `example.com`, oder eine Subdomäne, wie z. B. `blog.example.com`, der IPv4-Adresse eines Webservers oder einer Instance zu, wie z. B. `192.0.2.255`.

   1. Geben Sie im Textfeld Record name (Datensatzname) die Ziel-Unterdomain für den Datensatz oder ein @-Symbol ein, um den Scheitelpunkt Ihrer Domain zu definieren.
   2. Geben Sie im Textfeld Resolves to (Verweist auf) die Ziel-IP-Adresse für den Datensatz ein, wählen Sie Ihre laufende Instance oder den konfigurierten Load Balancer. Wenn Sie eine laufende Instance auswählen, wird die öffentliche IP-Adresse dieser Instance automatisch hinzugefügt.
   3. Wählen Sie Ist ein AWS Ressourcenalias, um den Datenverkehr an Ihre Lightsail- und -AWSRessourcen weiterzuleiten, z. B. an eine Verteilung oder einen Container-Service. Sie können auch Datenverkehr von einem Eintrag in einer DNS-Zone zu einem anderen Eintrag weiterleiten.

> **Note**
>
> Wir empfehlen Ihnen, Ihrer Lightsail-Instance eine statische IP anzufügen und dann die statische IP als Wert auszuwählen, in den der Datensatz aufgelöst wird. Weitere Informationen finden Sie unter Erstellen einer statischen IP.

CAA-Datensätze

Ein AAAA-Datensatz ordnet eine Domain, wie beispielsweise `example.com` oder eine Subdomain, wie `blog.example.com`, der IPv6-Adresse eines Webservers oder einer Instance zu, wie z. B. `2001:0db8:85a3:0000:0000:8a2e:0370:7334`.

> **Note**
>
> Lightsail unterstützt keine statischen IPv6-Adressen. Wenn Sie Ihre Lightsail-Ressource löschen und eine neue Ressource erstellen oder IPv6 für dieselbe Ressource deaktivieren und erneut aktivieren, müssen Sie möglicherweise Ihren AAAA-Datensatz aktualisieren, um die neueste IPv6-Adresse für die Ressource widerzuspiegeln.

1. Geben Sie im Textfeld Record name (Datensatzname) die Ziel-Unterdomain für den Datensatz oder ein @-Symbol ein, um den Scheitelpunkt Ihrer Domain zu definieren.
2. Geben Sie im Textfeld Resolves to (Verweist auf) die Ziel-IPv6-Adresse für den Datensatz ein, wählen Sie Ihre laufende Instance oder den konfigurierten Load Balancer. Wenn Sie eine laufende Instance auswählen, wird die öffentliche IPv6-Adresse dieser Instance automatisch hinzugefügt.
3. Wählen Sie Ist ein AWS Ressourcenalias, um den Datenverkehr an Ihre Lightsail- und -AWSRessourcen weiterzuleiten, z. B. an eine Verteilung oder einen Container-Service. Sie können auch Datenverkehr von einem Eintrag in einer DNS-Zone zu einem anderen Eintrag weiterleiten.

Kanonischer Name, CNAME-Datensatz

Ein CNAME-Datensatz ordnet einen Alias oder eine Subdomain, wie beispielsweise `www.example.com`, einer anderen Domain, wie beispielsweise `example.com`, oder einer anderen Subdomain, wie `blog.example.com`, zu.

1. Geben Sie im Textfeld Record name (Datensatzname) die Subdomain für den Datensatz ein.
2. Geben Sie im Textfeld Route traffic to (Datenverkehr weiterleiten an) die Zieldomain für den Datensatz ein.

Mail Exchanger, MX-Datensatz

Ein MX-Datensatz ordnet eine Subdomain, wie beispielsweise `mail.example.com`, einer E-Mail-Serveradresse mit Werten für die Priorität zu, wenn mehrere Server definiert sind.

1. Geben Sie im Textfeld Record name (Datensatzname) die Subdomäne für den Datensatz ein.
2. Geben Sie im Textfeld Priority (Priorität) die Priorität für den Datensatz ein. Dies ist wichtig, wenn Sie Datensätze für mehrere Server hinzufügen.
3. Geben Sie im Textfeld Route traffic to (Datenverkehr weiterleiten an) die Zieldomäne für den Datensatz ein.

Service-Locator, SRV-Datensatz

Ein SRV-Datensatz ordnet eine Subdomain, wie beispielsweise `service.example.com`, einer Serviceadresse mit Werten für Priorität, Gewichtung und Portnummer zu. Telefonie oder Instant Messaging sind nur einige der Dienste, die typischerweise mit SRV-Datensätzen verbunden sind.

1. Geben Sie im Textfeld Record name (Datensatzname) die Subdomäne für den Datensatz ein.
2. Geben Sie im Textfeld Priority (Priorität) die Priorität für den Datensatz ein.
3. Geben Sie im Feld Weight (Gewichtung) eine relative Gewichtung für SRV-Datensätze mit derselben Priorität an.
4. Geben Sie im Textfeld Route traffic to (Datenverkehr weiterleiten an) die Zieldomäne für den Datensatz ein.
5. Geben Sie im Textfeld Port die Portnummer ein, über die eine Verbindung hergestellt werden kann.

Text, TXT-Datensatz

Ein TXT-Datensatz bildet eine Subdomain in Klartext ab. Sie erstellen TXT-Datensätze, um den Besitz Ihrer Domain für einen Dienstanbieter zu bestätigen.

1. Geben Sie im Textfeld Record name (Datensatzname) die Subdomäne für den Datensatz ein.

2. Geben Sie im Textfeld Responds with (Antwortet mit) die Antwort ein, die angezeigt wird, wenn die Subdomain abgefragt wird.

> **Note**
>
> Der Eingabetext muss nicht mit Anführungszeichen eingeschlossen werden.

3. Wenn Sie mit dem Hinzufügen des Datensatzes fertig sind, wählen Sie das Symbol Save (Speichern), um Ihre Änderungen zu speichern.

   Der Datensatz wird der DNS-Zone hinzugefügt. Wiederholen Sie die obigen Schritte, um mehrere Datensätze zur DNS-Zone Ihrer Domain hinzuzufügen.

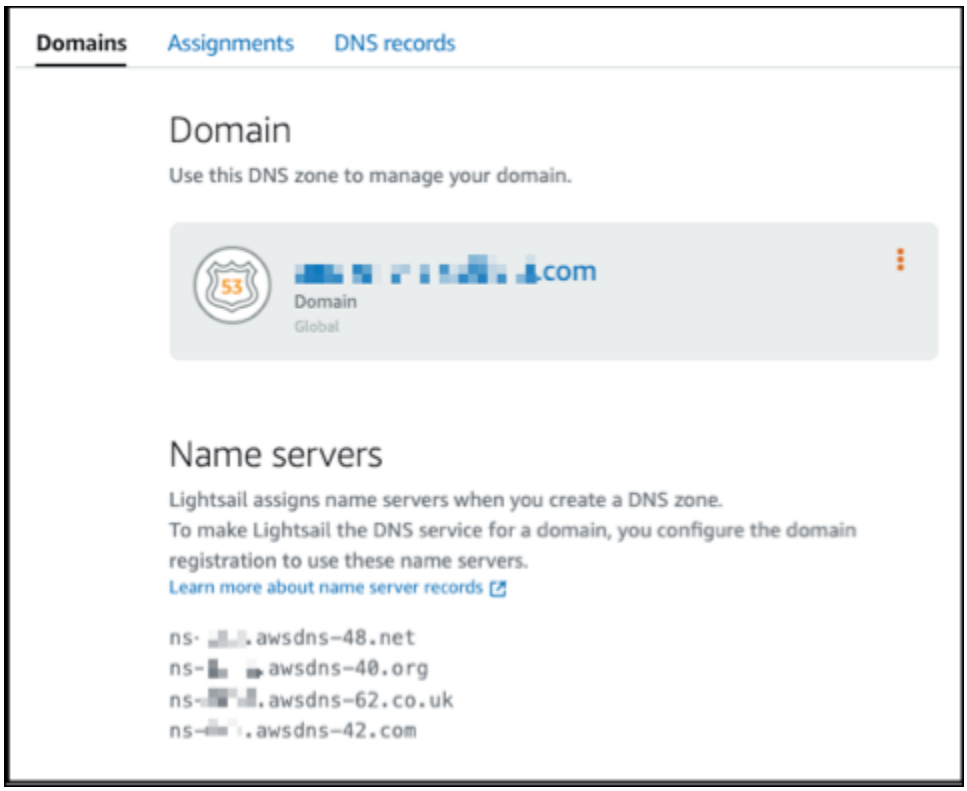
> **Note**
>
> Time to Live (TTL) für DNS-Datensätze kann in der Lightsail-DNS-Zone nicht konfiguriert werden. Stattdessen verwenden alle Lightsail-DNS-Datensätze standardmäßig eine TTL von 60 Sekunden. Weitere Informationen finden Sie unter Time to Live in Wikipedia.

Schritt 4: Ändern des Nameservers beim aktuellen DNS-Hosting-Provider Ihrer Domain

Führen Sie die folgenden Schritte aus, um die Verwaltung der DNS-Datensätze Ihrer Domain an Lightsail zu übertragen. Dazu melden Sie sich auf der Website des aktuellen DNS-Hosting-Anbieters Ihrer Domain an und ändern die Namenserver Ihrer Domain in die Lightsail-Nameserver.

> **Important**
>
> Wenn Webdatenverkehr derzeit an Ihre Domain weitergeleitet wird, stellen Sie sicher, dass alle vorhandenen DNS-Datensätze in der Lightsail-DNS-Zone vorhanden sind, bevor Sie die Namenserver beim aktuellen DNS-Hosting-Anbieter Ihrer Domain ändern. Auf diese Weise fließt der Datenverkehr kontinuierlich ohne Unterbrechung nach der Übertragung in die Lightsail-DNS-Zone.

1. Schreiben Sie sich die Lightsail-Nameserver auf, die auf der DNS-Zonenverwaltungsseite Ihrer Domain aufgeführt sind. Die Namenserver befinden sich auf der Registerkarte Domains Ihrer Lightsail-DNS-Zone.



2. Melden Sie sich auf der Website des aktuellen DNS-Hosting-Providers Ihrer Domain an.
3. Suchen Sie die Seite, auf der Sie die Nameserver Ihrer Domain bearbeiten können.

   Weitere Informationen zum Auffinden dieser Seite finden Sie in der Dokumentation des aktuellen DNS-Hosting-Providers Ihrer Domain.
4. Geben Sie die Lightsail-Nameserver ein und entfernen Sie andere aufgelistete Nameserver.
5. Speichern Sie Ihre Änderungen.

   Lassen Sie der Änderung der Nameserver Zeit, sich über das DNS des Internets zu verbreiten, was mehrere Stunden dauern kann. Nachdem dies abgeschlossen ist, sollte der Internetverkehr für Ihre Domäne über die Lightsail DNS-Zone geleitet werden.

Nächste Schritte

- Bearbeiten oder Löschen einer DNS-Zone
- Erstellen eines Load Balancers und Anfügen von Instances

Bearbeiten oder Löschen einer DNS-Zone in Lightsail

Sie können die DNS-Datensätze in der DNS-Zone Ihrer Domäne hinzufügen, bearbeiten oder löschen. Sie können die DNS-Zone Ihrer Domäne auch in Amazon Lightsail löschen, wenn Sie die Verwaltung der DNS-Datensätze Ihrer Domäne an einen anderen DNS-Hosting-Provider oder zurück an die Vergabestelle übertragen möchten, bei der Sie Ihre Domäne registriert haben.

> **Note**
>
> Bevor Sie Datensätze mit dem DNS-Editor in der Lightsail-Konsole bearbeiten können, müssen Sie die Verwaltung der DNS-Datensätze Ihrer Domäne auf Lightsail übertragen. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.

Bearbeiten Sie DNS-Datensätze

Sie können die DNS-Datensätze für die DNS-Zone Ihrer Domäne jederzeit über die Lightsail-Konsole bearbeiten.

So bearbeiten Sie die DNS-Zone

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie die Registerkarte Domains & DNS (Domänen und DNS) und dann den Namen der DNS-Zone, die Sie bearbeiten möchten.
3. Wählen Sie auf der Seite DNS records (DNS-Datensätze) eine der folgenden Optionen aus:
   - Um einen neuen Datensatz hinzuzufügen, wählen Sie Add record (Datensatz hinzufügen) aus.
   - Um einen bestehenden Datensatz zu bearbeiten, wählen Sie das Symbol Edit (Bearbeiten) neben dem Datensatz aus, den Sie bearbeiten möchten.
   - Um einen bestehenden Datensatz zu löschen, wählen Sie das Symbol Delete (Löschen) neben dem Datensatz aus, den Sie löschen möchten.
4. Wenn Sie fertig sind, wählen Sie das Symbol Save (Speichern), um Ihre Änderungen zu speichern.

> **Note**
>
> Warten Sie einige Zeit, damit sich die Änderungen an den DNS-Einträgen über das DNS im Internet ausbreiten, was mehrere Stunden dauern kann.

Eine DNS-Zone löschen

Sie können die DNS-Zone Ihrer Domäne auch in Lightsail löschen.

> **Important**
>
> Wenn Sie planen, den Traffic durch Ihre Domäne weiterzuleiten, bereiten Sie einen anderen DNS-Hosting-Provider vor, bevor Sie die DNS-Zone Ihrer Domäne in Lightsail löschen. Andernfalls stoppt der gesamte Traffic auf Ihrer Website, wenn Sie die Lightsail-DNS-Zone löschen.

So löschen Sie eine DNS-Zone

1. Wählen Sie auf der Startseite der Lightsail-Konsole die Registerkarte Domains & DNS (Domänen und DNS).
2. Klicken Sie auf den Namen der DNS-Zone, die Sie löschen möchten.
3. Wählen Sie das Menü mit senkrechten Ellipsen (⋮). Wählen Sie dann die Option Delete (Löschen) aus.
4. Wählen Sie zum Bestätigen des Löschvorgangs Delete DNS zone (DNS-Zone löschen).

   Die DNS-Zone wird aus Lightsail gelöscht.

Wie Internetdatenverkehr in Lightsail an Ihre Website weitergeleitet wird

Alle Computer im Internet, einschließlich Smartphones, Laptops und Website-Server, kommunizieren miteinander, indem sie eindeutige Zeichenfolgen verwenden. Diese Zeichenfolgen, bekannt als IP-Adressen, liegen in einem der folgenden Formate vor:

- Internetprotokoll Version 4 (IPv4), z. B. 192.0.2.44

- Internetprotokoll Version 6 (IPv6), z. B. 2001:DB8::/32

Wenn Sie einen Browser öffnen und eine Website aufrufen, müssen Sie sich nicht eine lange Zeichenfolge merken und eingeben. Stattdessen können Sie einen Domainnamen wie example.com eingeben und trotzdem an der richtigen Stelle ankommen. Dies wird durch das Domain Name System (DNS) erreicht, das als Verzeichnis fungiert, das registrierte Domainnamen auf IP-Adressen abbildet.

Inhalt

Übersicht über das Konfigurieren von Lightsail, um Internetdatenverkehr an Ihre Domain weiterzuleiten

In dieser Übersicht wird veranschaulicht, wie Sie Lightsail verwenden, um eine Domain zu registrieren und zu konfigurieren, die Internetdatenverkehr an Ihre Website oder Webanwendung weiterleitet.

1. Registrieren Sie den Domain-Namen. Eine Übersicht finden Sie unter Domainregistrierung.
2. Nachdem Sie Ihren Domainnamen registriert haben, erstellt Lightsail automatisch eine DNS-Zone, die denselben Namen wie die Domain trägt.
3. Mit der Lightsail-Konsole können Sie einer Lightsail-Ressource, z. B. einer Instance oder einem Load Balancer, einfach eine Domain zuweisen. Sie können auch DNS-Datensätze in Ihrer DNS-Zone erstellen, um den Datenverkehr an Ihre Ressourcen weiterzuleiten. Jeder Datensatz enthält Informationen darüber, wie Sie den Datenverkehr für Ihre Domain weiterleiten möchten, z. B. die folgenden:

   Name

   Der Name des Datensatzes entspricht dem Domainnamen (example.com) oder Subdomainnamen (www.example.com, retail.example.com). Der Name jedes Datensatzes in einer DNS-Zone muss mit dem Namen der DNS-Zone enden. Wenn der Name der DNS-Zone beispielsweise auf example.com endet, müssen alle Datensatznamen auf example.com enden.

   Typ

Der Datensatztyp hängt in der Regel vom Typ der Ressource ab, an die der Datenverkehr weitergeleitet werden soll. Wenn Sie beispielsweise den Datenverkehr an einen E-Mail-Server weiterleiten möchten, geben Sie MX als Typ ein. Um Datenverkehr für Ihren Domainnamen an Ihre Lightsail-Instance weiterzuleiten, fügen Sie einen A-Datensatz hinzu, der Ihren Domainnamen auf die statische IPv4-Adresse Ihrer Instance verweist, oder einen AAAA-Datensatz, der auf die IPv6-Adresse Ihrer Instance verweist.

4. Ziel

   Das Ziel ist der Ort, an den der Datenverkehr weitergeleitet werden soll. Sie können Aliasdatensätze erstellen, die den Datenverkehr an Lightsail-Instances, Lightsail-Container-Services und andere Lightsail-Ressourcen weiterleiten. Weitere Informationen finden Sie unter DNS.

So wird Datenverkehr für Ihre Domain weitergeleitet

Nach der Konfiguration von Lightsail zur Weiterleitung des Internetdatenverkehrs an Ihre Ressourcen, wie z. B. Instances, Load Balancer, Verteilungen oder Container-Services, geschieht Folgendes, wenn ein Benutzer Inhalte für www.example.com anfordert.

1. Ein Benutzer öffnet einen Webbrowser, gibt www.example.com in die Adresszeile ein und drückt die Eingabetaste.
2. Die Anforderung für www.example.com wird an einen DNS-Resolver weitergeleitet, der in der Regel vom Internetdienstanbieter (ISP) des Benutzers verwaltet wird. ISPs können Kabelanbieter, DSL-Breitbandanbieter oder Unternehmensnetzwerke sein.
3. Der DNS-Resolver des ISP leitet die Anforderung für www.example.com an einen DNS-Stamm-Namenserver weiter.
4. Der DNS-Resolver leitet die Anforderung von www.example.com erneut weiter, diesmal an einen der TLD-Namenserver für .com-Domains. Der Namensserver für .com-Domains beantwortet die Anforderung mit den Namen der vier Namenserver, die der Domain example.com zugeordnet sind.

   Der DNS-Resolver speichert die vier -Namensserver im Cache. Wenn ein Benutzer das nächste Mal example.com aufruft, überspringt der Resolver die Schritte 3 und 4, weil die Namenserver für example.com bereits ermittelt wurden. Die Namenserver werden in der Regel für zwei Tage im Zwischenspeicher gehalten.
5. Der DNS-Resolver wählt einen -Namenserver aus und leitet die Anforderung von www.example.com an diesen Namenserver weiter.

6. Der Namenserver sucht in der DNS-Zone von example.com nach dem Datensatz für www.example.com und ruft den zugehörigen Wert ab, z. B. die IP-Adresse für einen Webserver (192.0.2.44). Dann gibt der Namenserver die IP-Adresse an den DNS-Resolver zurück.
7. Der DNS-Resolver verfügt schließlich über die IP-Adresse, die der Benutzer benötigt. Der Auflöser gibt den Wert an den Webbrowser zurück.
8. Der Webbrowser sendet eine Anforderung für www.example.com an die IP-Adresse, die er vom DNS-Resolver erhalten hat. Dort befindet sich Ihr Inhalt, beispielsweise ein Webserver, der auf einer Lightsail-Instance ausgeführt wird, oder ein Container-Service, der als Website-Endpunkt konfiguriert ist.
9. Der Webserver bzw. die jeweilige Ressource unter 192.0.2.44 gibt die Webseite für www.example.com an den Webbrowser zurück, und der Webbrowser zeigt die Seite an.

Nächste Schritte

- DNS
- Verweisen Ihrer Domain auf eine Instance
- Verweisen Ihrer Domain auf einen Load Balancer
- Verweisen Sie Ihre Domain auf eine Verteilung

Verweisen Ihrer Lightsail-Domain auf eine Instance

Sie können die DNS-Zone in Amazon Lightsail verwenden, um einen registrierten Domänennamen wie example.com auf Ihre Website zu verweisen, die auf einer Lightsail-Instance ausgeführt wird, die auch als Virtual Private Server (VPS) bezeichnet wird. Sie können bis zu sechs DNS-Zonen in Ihrem Lightsail-Konto erstellen. Nicht alle DNS-Datensatztypen werden unterstützt. Weitere Informationen über Lightsail-DNS-Zonen finden Sie unter DNS.

Wenn Sie davon ausgehen, mehr als sechs DNS-Zonen zu erstellen oder DNS-Datensatztypen zu verwenden, die in Lightsail nicht unterstützt werden, empfehlen wir die Verwendung einer gehosteten Zone von .Amazon Route 53. Mit Route 53, können Sie das DNS für bis zu 500 Domains verwalten. Die Anwendung unterstützt auch eine größere Vielfalt von DNS-Datensatztypen. Weitere Informationen finden Sie unter Arbeiten mit gehosteten Zonen im Entwicklerhandbuch für Amazon Route 53.

In dieser Anleitung wird beschrieben, wie Sie die DNS-Datensätze für eine in Lightsail verwaltete Domain bearbeiten können, damit diese auf Ihre Lightsail-Instance verweist. Es kann bis zu 48 Stunden dauern, bis Änderungen an der DNS-Zone über das DNS im Internet verbreitet werden.

Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies nicht ohnehin bereits der Fall ist:

- Registrieren Sie einen Domänen-Namen mit Lightsail. Weitere Informationen finden Sie unter Registrieren einer neuen Domain.
- Wenn Sie bereits eine Domäne registriert haben, aber Lightsail nicht zur Verwaltung ihrer Datensätze verwenden, müssen Sie die Verwaltung der DNS-Datensätze für Ihre Domäne auf Lightsail übertragen. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.
- Die standardmäßig an Ihre Instance angefügte dynamische öffentliche IP-Adresse ändert sich bei jedem Stopp und Neustart der Lightsail-Instance. Erstellen Sie eine statische IP-Adresse und fügen Sie sie an Ihre Instance an, damit die öffentliche IP-Adresse nicht mehr geändert wird. In dieser Anleitung erstellen Sie einen DNS-Datensatz in der DNS-Zone Ihrer Domäne, der in die statische IP-Adresse aufgelöst wird. So müssen Sie nicht jedes Mal, wenn Sie Ihre Instance anhalten und neu starten, die DNS-Datensätze Ihrer Domäne aktualisieren. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

  Optional – Sie können IPv6 für Ihre Lightsail-Instance aktiviert belassen. Die IPv6-Adresse bleibt beim Anhalten und Starten Ihrer Instance bestehen. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren von IPv6.

Zuweisen einer Domäne zu einer Lightsail-Instance

Verwenden Sie eine der folgenden Methoden, um eine Domäne einer Instance in Lightsail zuzuweisen:

- Registerkarte „Domains“ (Domänen) für Instance
- Registerkarte „Domains“ (Domänen) für statische IP
- Registerkarte „Assignments“ (Zuweisungen) für DNS-Zone

Registerkarte „Domains“ (Domänen) für Instance

Gehen Sie wie folgt vor, um Ihre Domäne einer Lightsail-Instance auf der Registerkarte Domains (Domänen) für eine Instance der Lightsail-Konsole zuzuweisen.

So weisen Sie Ihre Domäne über die Registerkarte Domains (Domänen) der Instance zu

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie den Namen der Instance, der Sie die Domäne zuweisen möchten.
3. Wählen Sie auf der Registerkarte Domains (Domänen) die Option Assign domain (Domäne zuweisen) aus.
4. Wählen Sie die Domäne aus, die Sie Ihrer Lightsail-Instance zuweisen möchten.
5. Stellen Sie sicher, dass die Routing-Informationen korrekt sind, und wählen Sie dann Assign (Zuweisen) aus.

Optional

Um Ihre Domänenzuweisung in der Instance zu bearbeiten oder daraus zu entfernen, wählen Sie das Bearbeiten- oder Mülleimersymbol neben dem Domänennamen aus.

Registerkarte „Domains“ (Domänen) für statische IP

Gehen Sie wie folgt vor, um Ihre Domäne einer Lightsail-Instance auf der Registerkarte Domains (Domänen) für eine statische IP der Lightsail-Konsole zuzuweisen.

So weisen Sie Ihre Domäne über die entsprechende Registerkarte Domains (Domänen) zu

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie die Registerkarte Network (Network) aus.
3. Wählen Sie die statische IP aus, der Sie die Domäne zuweisen möchten.
4. Wählen Sie auf der Registerkarte Domains (Domänen) die Option Assign domain (Domäne zuweisen) aus.
5. Wählen Sie die Domäne aus, die Sie Ihrer statischen IP zuweisen möchten.
6. Stellen Sie sicher, dass die Routing-Informationen korrekt sind, und wählen Sie dann Assign (Zuweisen) aus.

Optional

Um Ihre Domänenzuweisung in der statischen IP zu bearbeiten oder daraus zu entfernen, wählen Sie das Bearbeiten- oder Mülleimersymbol neben dem Domänennamen aus.

Registerkarte „DNS zone assignments“ (DNS-Zonenzuweisungen)

Gehen Sie wie folgt vor, um Ihre Domäne einer Lightsail-Instance auf der Registerkarte Assignments (Zuweisungen) für eine DNS-Zone zuzuweisen.

So weisen Sie Ihre Domäne über die Registerkarte Assignments (Zuweisungen) zu

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie die Registerkarte Domains & DNS (Domänen und DNS).
3. Wählen Sie die DNS-Zone für den Domänennamen aus, den Sie verwenden möchten.
4. Wählen Sie auf der Registerkarte Assignments (Zuweisungen) die Option Add assignment (Zuweisung hinzufügen) aus.
5. Wählen Sie den Domänennamen aus, den Sie Ihrer Lightsail-Instance zuweisen möchten. Wenn der Instance noch keine statische IP zugewiesen ist, werden Sie aufgefordert, eine anzufügen.
6. Stellen Sie sicher, dass die Routing-Informationen korrekt sind, und wählen Sie dann Assign (Zuweisen) aus.

Optional

Um Ihre Domänenzuweisung in der Ressource zu bearbeiten oder daraus zu entfernen, wählen Sie das Bearbeiten- oder Mülleimersymbol neben dem Domänennamen aus.

Verweisen Ihrer Lightsail-Domain auf einen Load Balancer

Nachdem Sie überprüft haben, dass Sie die Domäne, in der Sie den Datenverkehr (HTTPS) verschlüsseln möchten, kontrollieren, müssen Sie einen Adressen- (A) Datensatz dem DNS-Hostinganbieter Ihrer Domäne hinzufügen, der Ihre Domäne zu Ihrem Lightsail Load Balancer verweist. In diesem Leitfaden zeigen wir Ihnen, wie Sie den A-Datensatz einer Lightsail-DNS-Zone und einer gehosteten Zone in Amazon Route 53 hinzufügen.

Mithilfe der Seite „DNS zone - Assignments (DNS-Zone – Zuweisungen)“ einen A-Datensatz hinzufügen

1. Wählen Sie auf der Lightsail-Startseite Domains & DNS (Domänen & DNS) aus.

2. Wählen Sie die DNS-Zone aus, die Sie verwalten möchten.
3. Wählen Sie die Registerkarte Assignments (Zuweisungen).
4. Wählen Add assignment (Zuweisung hinzufügen) aus.
5. Wählen Sie im Feld Select a domain name (Domainnamen auswählen) aus, ob Sie den Domainnamen oder eine Subdomain der Domain verwenden möchten.
6. Wählen Sie in der Dropdownliste Select a resource (Ressource auswählen) den Load Balancer aus, dem Sie die Domain zuweisen möchten.
7. Wählen Sie Assign (Zuweisen).

Warten Sie einige Zeit, damit sich die Änderung über das DNS im Internet ausbreitet. Dieser Vorgang kann zwischen einigen Minuten und mehreren Stunden dauern.

Mithilfe der Seite „DNS zone - DNS recors (DNS-Zone – DNS-Datensätze)“ einen A-Datensatz hinzufügen

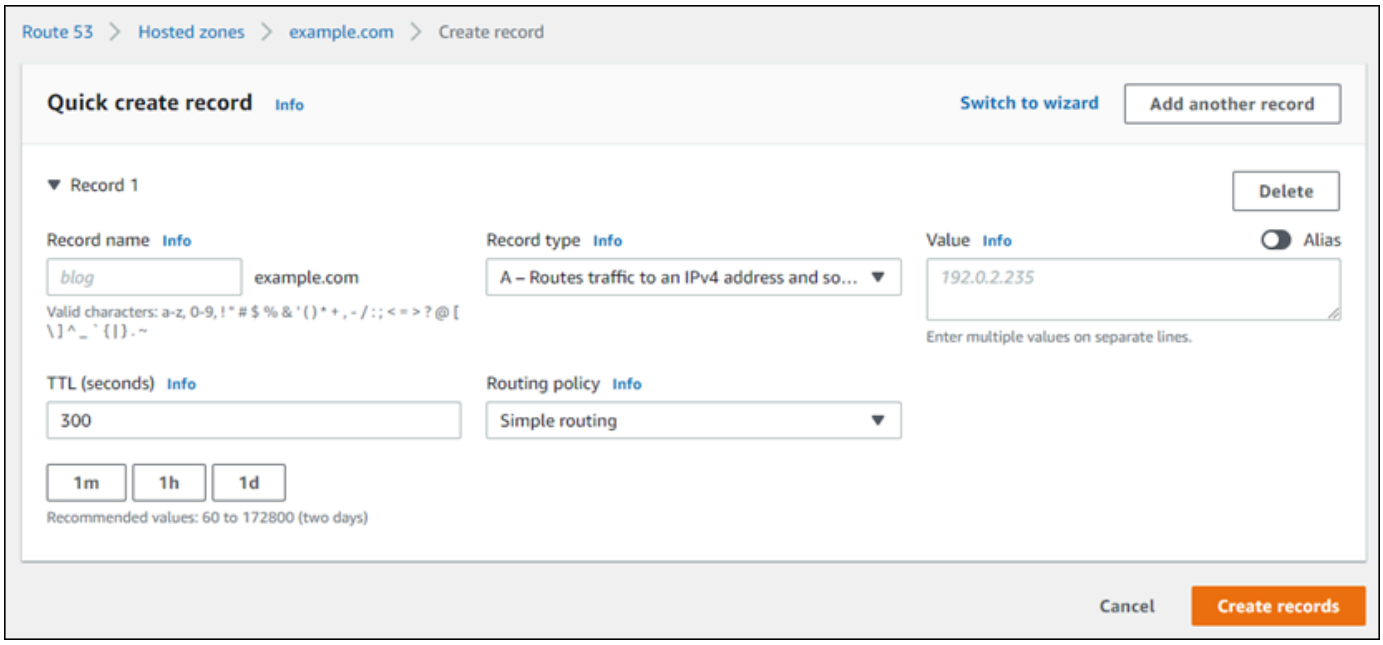
1. Wählen Sie auf der Lightsail-Startseite Domains & DNS (Domänen & DNS) aus.
2. Wählen Sie die DNS-Zone aus, die Sie verwalten möchten.
3. Wählen Sie die Registerkarte DNS records (DNS-Datensätze) aus.
4. Führen Sie je nach aktuellem Status Ihrer DNS-Zone einen der folgenden Schritte aus:
   - Wenn Sie keinen A-Datensatz hinzugefügt haben, wählen Sie Datensatz hinzufügen aus.
   - Wenn Sie zuvor einen A-Datensatz hinzugefügt haben, klicken Sie neben dem bestehenden A-Datensatz, der auf der Seite aufgeführt ist, auf das Symbol „Bearbeiten“, und springen Sie dann auf Schritt 5 dieses Vorgangs.
5. Wählen Sie A-Datensatz im Dropdown-Menü für die Datensatzart aus.
6. Geben Sie im Textfeld Record name (Datensatzname) eine der folgenden Optionen ein:
   - Geben Sie `@` ein, um den Datenverkehr für die Spitze Ihrer Domäne (z. B. `example.com`) an Ihren Load Balancer weiterzuleiten.
   - Geben Sie `www` ein, um den Datenverkehr für die www-Unterdomäne (z. B. `www.example.com`) an Ihren Load Balancer weiterzuleiten.
7. Wählen Sie im Textfeld Überträgt auf den Namen Ihres Lightsail-Load-Balancers aus.
8. Wählen Sie Speichern.

Warten Sie einige Zeit, damit sich die Änderung über das DNS im Internet ausbreitet. Dieser Vorgang kann zwischen einigen Minuten und mehreren Stunden dauern.

Einen A-Datensatz in Route 53 hinzufügen

1. Melden Sie sich bei der Route-53-Konsole an.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie die gehostete Zone für den Domänennamen aus, den Sie verwenden möchten, um den Datenverkehr an den Load Balancer weiterzuleiten.
4. Wählen Sie Datensatz erstellen.

   Die Seite Datensatz schnell erstellen wird angezeigt.



> **Note**
>
> Wenn Ihnen die Seite Routing-Richtlinie auswählen angezeigt wird, wählen Sie dann Auf schnell erstellen wechseln, um zum Schnellerstellungsassistenten zu wechseln, bevor Sie mit den folgenden Schritten fortfahren.

5. Als Datensatzname geben Sie `www` ein, wenn Sie planen, die `www`-Unterdomäne (d. h. `www.example.com`) zu verwenden, oder lassen Sie das Feld leer, wenn Sie die Spitze der Domäne verwenden möchten (d. h. `example.com`).

6. Wählen Sie für Datensatzart A – Leitet Datenverkehr an eine IPv4-Adresse und einige AWS-Ressourcen weiter.
7. Wählen Sie den Schalter Alias aus, um Alias-Datensätze zu aktivieren.
8. Wählen Sie die folgenden Optionen für Datenverkehr weiterleiten an aus:

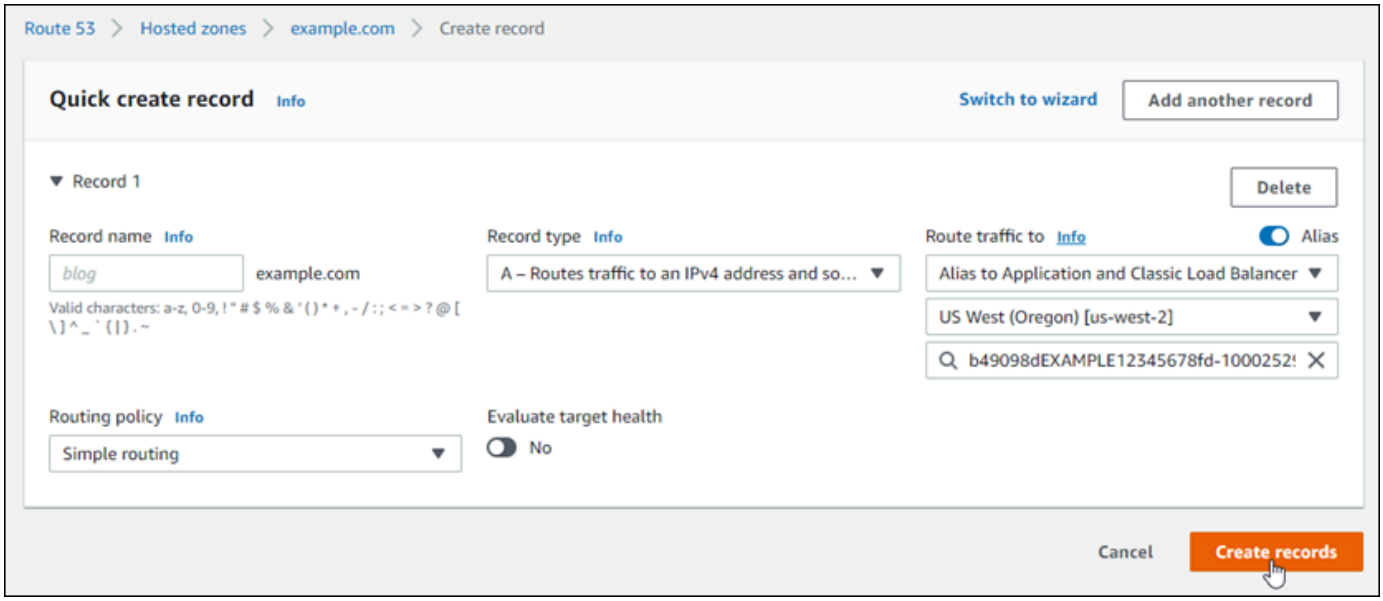
   a. Unter Endpunkt auswählen, wählen Sie Alias zur Anwendung und Classic Load Balancer aus.

   b. Unter Region auswählen wählen Sie die AWS-Region aus, in der Sie Ihren Lightsail-Load-Balancer erstellt haben.

   c. Unter Load Balancer auswählen geben Sie die Endpunkt-URL (d. h. DNS-Name) Ihres Lightsail-Load-Balancers ein oder kopieren Sie diese.
9. Unter Routing-Richtlinie wählen Sie Einfaches Routing und deaktivieren Sie den Schalter Zielzustand auswerten.

   Lightsail führt bereits Zustandsprüfungen für Ihren Load Balancer aus. Weitere Informationen finden Sie unter Zustandsprüfung für Ihren Load Balancer.

   Ihre Akte sollte wie im folgenden Beispiel aussehen.



10. Wählen Sie Akten erstellen, um die Akte zu Ihrer gehosteten Zone hinzuzufügen.

> **Note**
>
> Warten Sie einige Zeit, damit sich die Änderung über das DNS im Internet ausbreitet. Dieser Vorgang kann zwischen einigen Minuten und mehreren Stunden dauern.

Aktualisieren Ihrer Lightsail-Domainnamenserver, um einen anderen DNS-Service zu verwenden

Sie können eine Amazon Lightsail-DNS-Zone verwenden, um die DNS-Datensätze für eine Domäne zu verwalten, die Sie mit Lightsail registriert haben. Alternativ können Sie die Verwaltung der DNS-Datensätze für die Domäne an einen anderen DNS-Hosting-Anbieter übertragen. In diesem Handbuch zeigen wir Ihnen, wie Sie die Verwaltung von DNS-Datensätzen für eine Domäne, die Sie mit Lightsail registriert haben, an einen anderen DNS-Hosting-Anbieter übertragen.

> **Important**
>
> Die Verbreitung aller Änderungen, die Sie am DNS Ihrer Domäne vornehmen, über das DNS im Internet kann mehrere Stunden dauern. Aus diesem Grund sollten Sie die DNS-Datensätze Ihrer Domäne beim aktuellen DNS-Hosting-Provider Ihrer Domäne beibehalten, bis die Übertragung der Verwaltung abgeschlossen ist. Dadurch wird sichergestellt, dass der Datenverkehr für Ihre Domain während der Übertragung ununterbrochen zu Ihren Ressourcen weitergeleitet wird.

Inhalt

Sorgen Sie dafür, dass die Voraussetzungen erfüllt sind.

Erfüllen Sie die folgenden Voraussetzungen, wenn dies nicht ohnehin bereits der Fall ist:

1. Registrieren Sie einen Domainnamen Sie können einen Domänennamen mit Lightsail registrieren. Weitere Informationen finden Sie unter Registrieren einer neuen Domain.

2. Verwenden Sie den Prozess, der von Ihrem DNS-Service bereitgestellt wird, um die Namenserver für Ihre Domäne abzurufen.

Datensätze zur DNS-Zone hinzufügen

Führen Sie das folgende Verfahren aus, um die Namenserver für einen anderen DNS-Hosting-Anbieter Ihrer registrierten Domäne in Lightsail hinzuzufügen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie die Registerkarte Domains & DNS (Domänen und DNS).
3. Wählen Sie den Namen der Domäne aus, die Sie für einen anderen DNS-Service konfigurieren möchten.
4. Klicken Sie auf Edit Name Servers (Namenserver bearbeiten).
5. Ändern Sie die Namen der Namenserver in die Namenserver, die Sie vom DNS-Service erhalten haben, als Sie die Voraussetzungen erfüllt haben.
6. Wählen Sie Save (Speichern).

Verwenden von Amazon Route 53, um eine Domain auf eine Lightsail Instance zu verweisen

Durch die DNS-Zone in Amazon Lightsail ist es ganz einfach, einen registrierten Domänennamen, wie z. B. `example.com`, auf Ihre Website zu verweisen, die auf einer Lightsail-Instance ausgeführt wird. Sie können bis zu sechs Lightsail-DNS-Zonen erstellen und nicht alle DNS-Datensatztypen werden unterstützt. Weitere Informationen über Lightsail-DNS-Zonen finden Sie unter DNS.

Wenn die Lightsail-DNS-Zone für Sie zu begrenzt ist, empfehlen wir die Verwendung einer gehosteten Zone von Amazon Route 53 zum Verwalten der DNS-Datensätze Ihrer Domain. Sie können das DNS für bis zu 500 Domains mit Route 53 verwalten und es wird eine größere Bandbreite an DNS-Datentypen unterstützt. Oder Sie verwenden bereits Route 53, um die DNS-Datensätze Ihrer Domain zu verwalten und möchten es weiterhin verwenden. In dieser Anleitung wird beschrieben, wie Sie die DNS-Datensätze für eine in verwaltete Domain bearbeiten können, um auf Ihre Lightsail-Instance zu verweisen.

Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies nicht ohnehin bereits der Fall ist:

- Registrieren neuer Domainnamen mithilfe von Amazon Route 53. Weitere Informationen finden Sie unter Registrieren einer neuen Domain in der Route-53-Dokumentation.
- Wenn Sie bereits eine Domain registriert haben, aber Route 53 nicht zur Verwaltung ihrer Datensätze verwenden, müssen Sie die Verwaltung der DNS-Datensätze für Ihre Domain auf Route 53 übertragen. Weitere Informationen finden Sie unter Amazon Route 53 zum DNS-Service für eine vorhandene Domain machen.
- Erstellen Sie eine öffentlich gehostete Zone für Ihre Domain in Route 53. Weitere Informationen finden Sie unter Erstellen einer öffentlich gehosteten Zone in der Route-53-Dokumentation.
- Erstellen Sie eine statische IP-Adresse und ordnen Sie sie Ihrer Lightsail-Instance zu. In dieser Anleitung erstellen Sie einen DNS-Eintrag in der von Route 53 gehosteten Zone Ihrer Domain, der zur statischen IP-Adresse (öffentliche IP-Adresse) Ihrer Instance aufgelöst wird. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

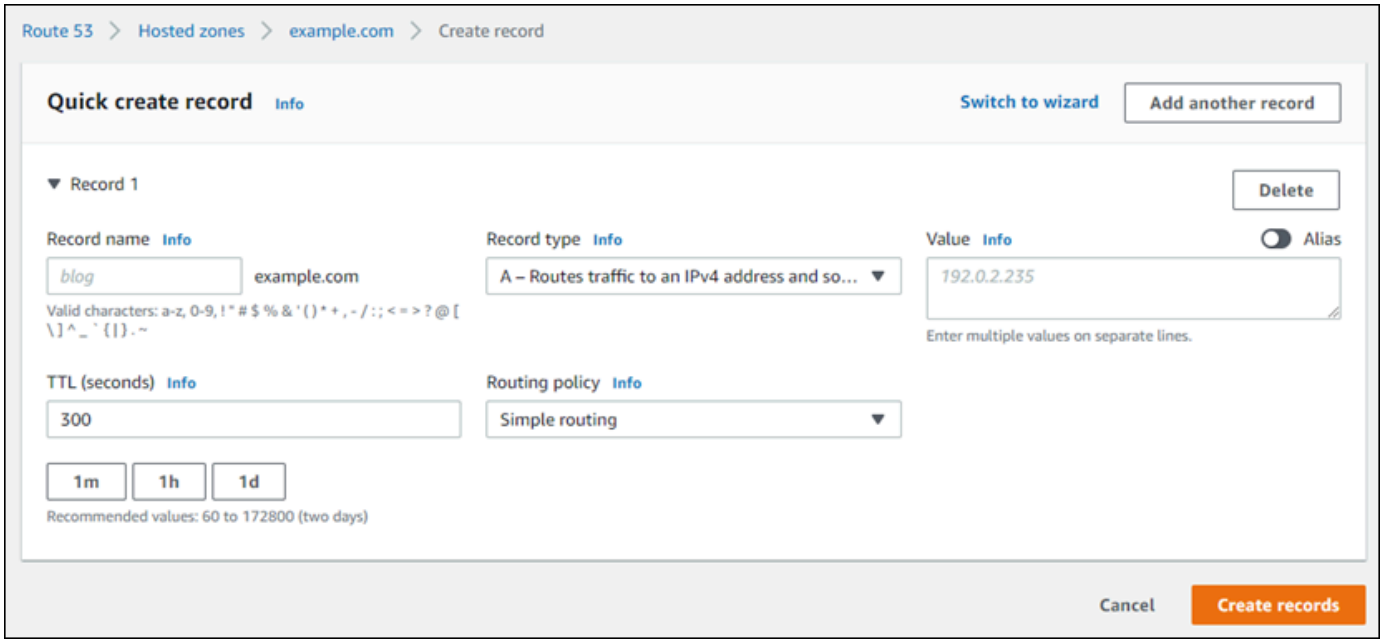
Verweisen einer Domain auf eine Lightsail-Instance mit Route 53

Führen Sie die folgenden Schritte aus, um die beiden häufigsten DNS-Einträge, die Adresse und den kanonischen Namen in Route 53 zu konfigurieren, um Ihre Domain auf eine Lightsail-Instance zu verweisen.

> **Note**
>
> Dieses Verfahren ist auch im Route-53-Entwicklerhandbuch dokumentiert. Für weitere Informationen sehen Sie Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole in der Route-53-Dokumentation.

1. Melden Sie sich bei der Route-53-Konsole an.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie die gehostete Zone für den Domänennamen aus, den Sie verwenden möchten, um den Datenverkehr an den Load Balancer weiterzuleiten.
4. Wählen Sie Datensatz erstellen.

   Die Seite Datensatz schnell erstellen wird angezeigt.



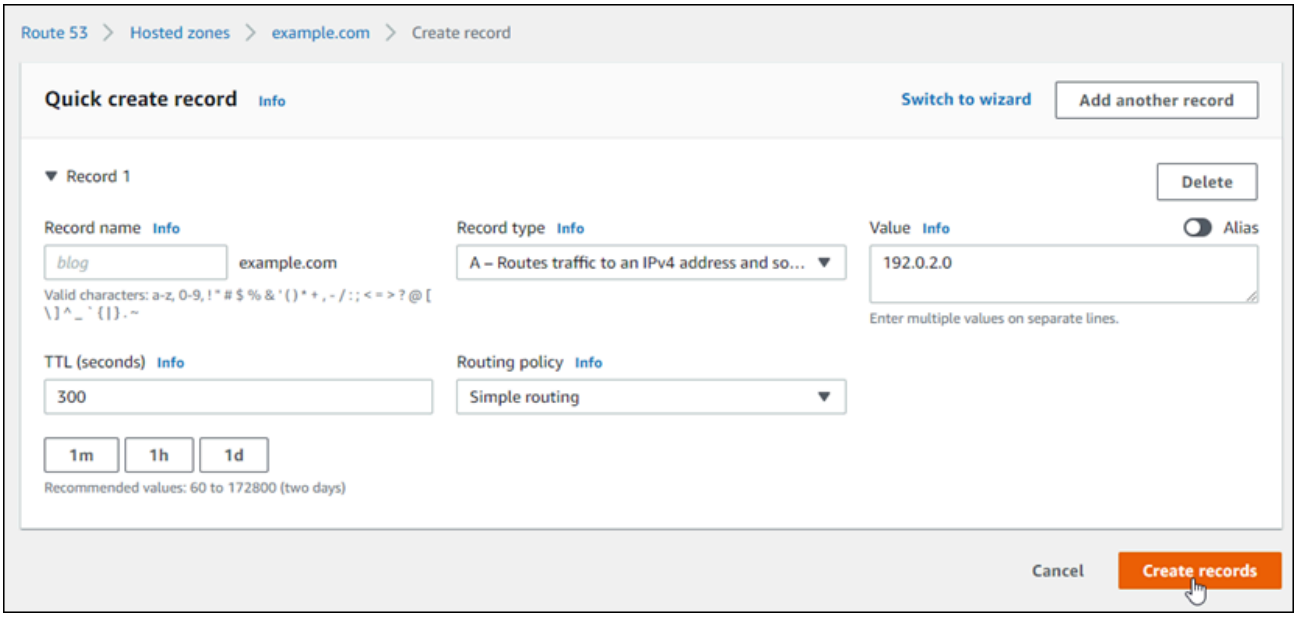
> **Note**
>
> Wenn Ihnen die Seite Routing-Richtlinie auswählen angezeigt wird, wählen Sie dann Auf schnell erstellen wechseln, um zum Schnellerstellungsassistenten zu wechseln, bevor Sie mit den folgenden Schritten fortfahren.

5. Wählen Sie bei Regionen eine der folgenden Optionen aus:

A – Leitet Datenverkehr an eine IPv4-Adresse und einige AWS-Ressourcen weiter

Ein (A) Adressendatensatz ordnet eine Domäne, wie beispielsweise `example.com` oder eine Subdomäne, wie `blog.example.com`, der IP-Adresse eines Webservers, wie `192.0.2.255` zu.

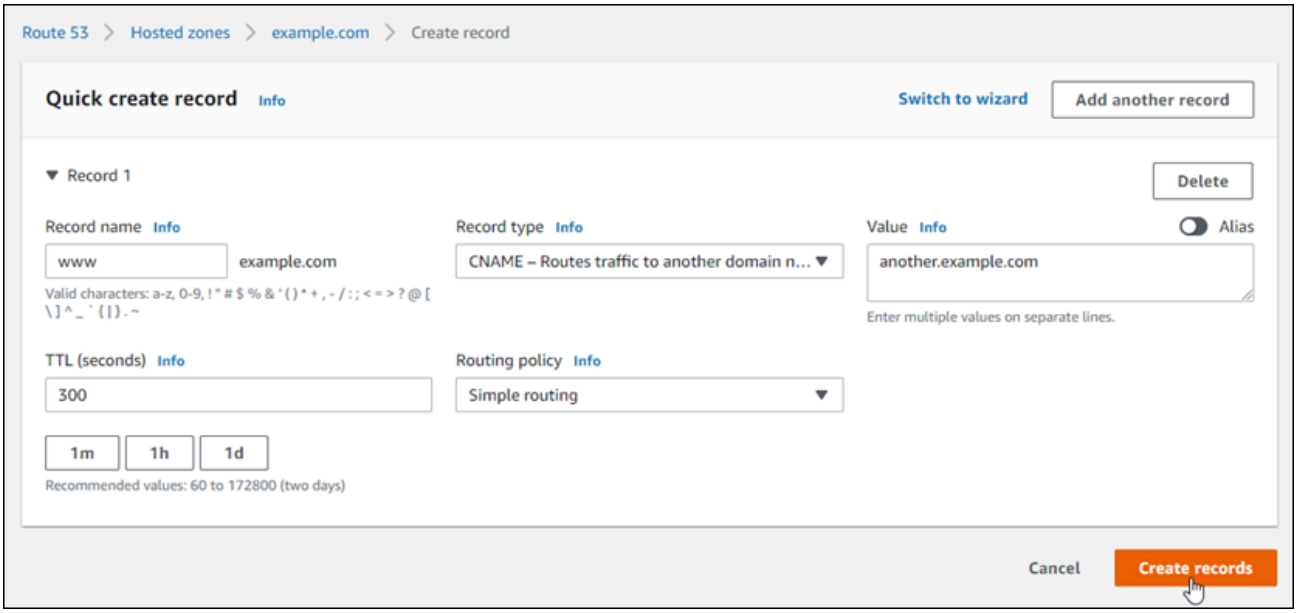
1. Halten Sie das Textfeld Name leer, damit der Apex Ihrer Domäne, z. B. `example.com`, auf die IP-Adresse verweist, oder geben Sie eine Subdomäne an.
2. Wählen A – Leitet Datenverkehr an eine IPv4-Adresse und einige AWS-Ressourcen weiter im Dropdown-Menü Datensatzart.
3. Geben Sie die statische IP-Adresse (öffentliche IP-Adresse) Ihrer Lightsail-Instance in das Textfeld Value (Wert) ein.
4. Behalten Sie die TTL von 300 und die Routing-Richtlinie als Einfaches Routing.



CNAME – Leitet Datenverkehr an einen anderen Domänennamen und einige AWS-Ressourcen weiter

Ein kanonischer Name (CNAME)-Datensatz bildet einen Alias oder eine Subdomäne, wie z. B. `www.example.com`, auf eine Domäne, wie z. B. `example.com`, oder eine Subdomäne, wie z. B. `www2.example.com` ab. Ein CNAME-Datensatz leitet eine Domäne in eine andere um.

1. Geben Sie eine Subdomäne in das Textfeld Aktenname ein.
2. Wählen Sie CNAME – Leitet Datenverkehr an einen anderen Domänennamen und einige AWS-Ressourcen im Dropdown-Menü Datensatztyp.
3. Geben Sie eine Domäne (z. B. `example.com`) oder Subdomäne (z. B. `another.example.com`) in das Textfeld Wert ein.
4. Behalten Sie die TTL von 300 und die Routing-Richtlinie als Einfaches Routing.



6. Wählen Sie Akten erstellen, um die Akte zu Ihrer gehosteten Zone hinzuzufügen.

> **Note**
>
> Warten Sie einige Zeit, damit sich die Änderung über das DNS im Internet ausbreitet. Dieser Vorgang kann zwischen einigen Minuten und mehreren Stunden dauern.

Um einen bestehenden Datensatz in der von Route 53 gehosteten Zone zu bearbeiten, wählen Sie den zu bearbeitenden Datensatz, geben Sie Ihre Änderungen ein und wählen Sie dann Speichern.

Registrieren einer neuen Domäne in Lightsail

Sie können einen Domainnamen mit Amazon Lightsail registrieren. Lightsail-Domains sind über Amazon Route 53, einen hochverfügbaren und skalierbaren DNS-Webservice registriert. Wenn Sie Domänen haben, die bei anderen Anbietern registriert sind, können Sie die DNS-Verwaltung dieser Domänen an Lightsail übertragen. Sie können diese Domänen auch auf Ihre Lightsail-Ressourcen verweisen.

Wählen Sie eines der folgenden Verfahren aus, um eine neue Domäne mit Lightsail zu registrieren:

- Informationen zum Registrieren einer neuen Domäne finden Sie unter Registrieren einer neuen Domäne mit Lightsail.

- Informationen für eine vorhandene Domain finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.
- Informationen zum Übertragen einer Domain an eine andere Vergabestelle finden Sie unter Verwalten einer Lightsail-Domain in Amazon Route 53.

Beachten Sie die folgenden Überlegungen zur Domänenregistrierung, bevor Sie beginnen:

Preise für Domänenregistrierung

Informationen zu den Kosten für die Registrierung von Domains finden Sie im Preisleitfaden für Amazon Route 53.

Domain Service Quotas

Es gibt ein Limit für die Anzahl der Domänen, die Sie registrieren können. Weitere Informationen finden Sie unter Service Quotas im Entwicklerhandbuch für Amazon Route 53. Wenn Sie das Limit erhöhen möchten, kontaktieren Sie Route 53.

Unterstützte Domänen

Lightsail unterstützt die Registrierung aller generischen Top-Level-Domänen (TLDs). Weitere Informationen zu den unterstützten TLDs finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können im Entwicklerhandbuch für Amazon Route 53.

Sie müssen Route 53 verwenden, um geografische Top-Level-Domains zu registrieren. Weitere Informationen finden Sie unter Geografische Top-Level-Domains im Entwicklerhandbuch für Amazon Route 53.

Domänennamen können nach der Registrierung nicht geändert werden.

Wenn Sie versehentlich einen falschen Domänennamen registrieren, können Sie diesen nicht mehr ändern. Stattdessen müssen Sie einen weiteren Domänennamen registrieren und dabei den richtigen Namen angeben. Es gibt keine Rückerstattungen für versehentlich registrierte Domänennamen.

Gebühren für DNS-Zonen

Wenn Sie eine Domain mit Lightsail registrieren, erstellen wir für die Domain automatisch eine DNS-Zone. Lightsail erhebt keine Gebühr für die DNS-Zone.

Registrieren einer neuen Domäne mit Lightsail

Inhalt

Erfüllen der Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies nicht ohnehin bereits der Fall ist:

1. Vergewissern Sie sich, dass die notwendigen DNS-Eintragstypen für Ihre Domain von der DNS-Zone in Lightsail unterstützt werden. Die Lightsail DNS-Zone unterstützt derzeit folgende Datentypen: Adresse (A), kanonischer Name (CNAME), Mail-Exchanger (MX), Nameserver (NS), Service Locator (SRV) und Text (TXT). Für NS-Einträge können Sie Wildcard-DNS-Datensätze verwenden.

   Wenn die erforderlichen DNS-Datensatztypen für Ihre Domain von der Lightsail-DNS-Zone nicht unterstützt werden, möchten Sie vielleicht Route 53 als DNS-Hosting-Anbieter für Ihre Domain verwenden. Route 53 unterstützt mehr Datensatztypen. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen und Amazon Route 53 als DNS-Service für eine bestehende Domain einrichten im Handbuch für Entwickler von Amazon Route 53.

Eine neue Domäne registrieren

So registrieren Sie eine neue Domäne

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie die Registerkarte Domains & DNS (Domänen und DNS).
3. Wählen Sie Register domain (Domäne registrieren) aus und geben Sie die Domäne ein, die Sie registrieren möchten.
   a. Geben Sie den Domänennamen ein, den Sie registrieren möchten, und klicken Sie auf Check availability (Verfügbarkeit prüfen), um herauszufinden, ob der Domänennamen verfügbar ist. Wenn die Domäne verfügbar ist, fahren Sie mit Automatic domain renewal (Automatische Domänenverlängerung) fort.

b. Wenn der Domänenname nicht verfügbar ist, werden andere Domänen aufgeführt, die Sie eventuell registrieren möchten (statt oder zusätzlich zu Ihrer ersten Auswahl). Wählen Sie Select (Auswählen) für die Domäne aus, die Sie registrieren möchten.

4. Geben Sie an, ob Ihre Domänenregistrierung vor dem Ablaufdatum automatisch verlängert werden soll. Wenn Sie einen Domänennamen registrieren, besitzen Sie ihn standardmäßig für ein Jahr. Wenn Sie Ihre Domänennamenregistrierung nicht verlängern, läuft sie ab und eine andere Person kann den Domänennamen registrieren. Um sicherzustellen, dass Sie Ihren Domänennamen behalten, können Sie ihn jedes Jahr automatisch verlängern lassen oder eine längere Laufzeit auswählen.
5. Geben Sie im Abschnitt Domain contact information (Domänenkontaktinformationen) die Kontaktinformationen für den Domänen-Registrierenden und den technischen und administrativen Kontakt an. Weitere Informationen finden Sie unter Angegebene Werte beim Registrieren oder Übertragen einer Domäne.

   Beachten Sie die folgenden Überlegungen:

   Vorname und Nachname

   Wir empfehlen für First Name (Vorname) und Last Name (Nachname) den Namen so einzugeben, wie er in Ihrem offiziellen Ausweis lautet. Für einige Änderungen an den Domäneneinstellungen erfordern manche Domänen-Registrierungen einen Identitätsnachweis. Der Name in Ihrer ID muss genau mit dem Namen des aktuellen Registrierenden der Domäne übereinstimmen.

   Unterschiedliche Kontakte

   Standardmäßig verwenden wir die gleichen Informationen für alle drei Kontakte. Wenn Sie andere Informationen für einen oder mehrere Kontakte eingeben möchten, deaktivieren Sie das Kontrollkästchen Same as registrant (Identisch mit dem Registrierenden) und geben Sie die neuen Kontaktinformationen ein.
6. Wählen Sie im Abschnitt Privacy protection (Datenschutz) aus, ob Sie Ihre Kontaktinformationen vor WHOIS-Anfragen verbergen möchten.

   Weitere Informationen finden Sie unter den folgenden Themen:

   - Datenschutz
   - Domains, die Sie mit Amazon Route 53 registrieren können

7. Wählen Sie Register domain (Domäne registrieren), um fortzufahren. Die Abschnitte DNS zones (DNS-Zonen) und Summary (Zusammenfassung) enthalten Informationen über die DNS-Zone der Domäne, die Preise und den Verlängerungsplan.
8. Sie müssen die Domainnamen-Registrierungsvereinbarung von Amazon Route 53 akzeptieren, bevor Sie Ihre Domain registrieren können.

Kontaktinformationen der Domäne überprüfen

Nach Registrierung der Domäne müssen Sie überprüfen, ob die E-Mail-Adresse für den Registrierenden-Kontakt gültig ist.

Anschließend wird automatisch eine Verifizierungs-E-Mail von einer der folgenden E-Mail-Adressen gesendet:

noreply@registrar.amazon.com

Für Domänen mit Amazon Registrar als Vergabestelle

noreply@domainnameverification.net

Für Domänen, deren Vergabestelle unsere Partner-Vergabestelle Gandi ist Informationen dazu, wie Sie die Vergabestelle für Ihre TLD ermitteln können, finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können im Handbuch für Entwickler von Amazon Route 53.

Gehen Sie wie folgt vor, um die Domänenverifizierung abzuschließen.

So schließen Sie die Verifizierung ab

1. Wenn Sie die Bestätigungs-E-Mail erhalten, wählen Sie den Link in der E-Mail, um zu bestätigen, dass die E-Mail-Adresse gültig ist. Wenn Sie die E-Mail nicht sofort erhalten, überprüfen Sie Ihren Spam-Ordner.
2. Kehren Sie zur Lightsail-Konsole zurück. Wenn der Status nicht automatisch in Verified (Verifiziert) aktualisiert wird, wählen Sie Refresh status (Status aktualisieren) aus.

> **Important**
>
> Der Registrierenden-Kontakt muss die Anweisungen in der E-Mail befolgen, um zu bestätigen, dass die E-Mail-Adresse empfangen wurde. Andernfalls wird die Domäne

gesperrt, wie von ICANN gefordert. Wenn eine Domäne gesperrt ist, kann im Internet nicht darauf zugegriffen werden.

3. Wenn die Domänenregistrierung abgeschlossen ist, wählen Sie, ob Sie Lightsail als Ihren DNS-Dienst oder einen anderen DNS-Dienst verwenden möchten.
   - Lightsail

     In der DNS-Zone, die Lightsail bei der Registrierung der Domäne erstellt hat, erstellen Sie Datensätze und teilen Lightsail mit, wie der Datenverkehr für die Domäne und Subdomänen weitergeleitet werden soll.

     Wenn zum Beispiel jemand den Domainnamen in einen Browser eingibt und diese Abfrage an Lightsail weitergeleitet wird, möchten Sie, dass Lightsail die Abfrage mit der IP-Adresse eines Webservers oder mit dem Namen eines Load Balancers beantwortet? Weitere Informationen finden Sie unter Bearbeiten oder Löschen einer DNS-Zone.
   - Verwenden eines anderen DNS-Service

     Konfigurieren Sie Ihre neue Domäne zum Weiterleiten von DNS-Abfragen an einen anderen DNS-Service als Lightsail. Weitere Informationen finden Sie unter So aktualisieren Sie die Namensserver für Ihre Domäne, wenn Sie einen anderen DNS-Service verwenden möchten.

So zeigen Sie Informationen zu Domain an, die bei Amazon Registrar registriert sind

Sie können Informationen zu .com-, .net- und .org-Domains anzeigen, die mit und Amazon Lightsail und Amazon Route 53 registriert wurden und für die Amazon Registrar die Vergabestelle ist. Diese Informationen umfassen Details, z. B. wann die Domäne ursprünglich registriert wurde, und Kontaktinformationen für den Domäneneigentümer sowie für die technischen und administrativen Kontakte.

Beachten Sie Folgendes:

E-Mail-Domainkontakte bei aktivem Datenschutz

Wenn der Datenschutz für die Domäne aktiv ist, werden Kontaktinformationen für den Registrierenden sowie technische und administrative Kontakte durch Kontaktinformationen für den Amazon Registrar-Datenschutz ersetzt. Wenn die Domäne example.com beispielsweise bei Amazon Registrar registriert ist und der Datenschutz aktiv ist, würde der Wert von

Registrant Email (E-Mail des Registrierenden) in der Antwort auf eine WHOIS-Abfrage `owner1234@example.com.whoisprivacyservice.org` ähneln.

Um bei aktivem Datenschutz mindestens einen Domänenkontakt zu kontaktieren, senden Sie eine E-Mail an die entsprechenden E-Mail-Adressen. Wir leiten Ihre E-Mail automatisch an den entsprechenden Ansprechpartner weiter.

Missbrauch melden

Um illegale Aktivitäten oder Verstöße gegen die Richtlinien für die zulässige Nutzung, einschließlich unangemessener Inhalte, Phishing, Malware oder Spam, zu melden, senden Sie eine E-Mail an abuse@amazon.com.

So zeigen Sie Informationen zu Domänen an, die bei Amazon Registrar registriert sind

1. Navigieren Sie in einem Webbrowser zu einer der folgenden Websites. Auf beiden Websites werden dieselben Informationen angezeigt. Sie verwenden jedoch unterschiedliche Protokolle und zeigen die Informationen in verschiedenen Formaten an:
   - WHOIS: https://registrar.amazon.com/whois
   - RDAP: https://registrar.amazon.com/rdap
2. Geben Sie den Namen der Domäne ein, zu der Sie Informationen anzeigen möchten, und wählen Sie Search (Suchen) aus. Wenn die von Ihnen gesuchte Domain nicht mit Amazon Lightsail oder Route 53 registriert wurde, wird Ihnen eine Meldung angezeigt, die besagt, dass die Domain nicht in der Vergabestelle-Datenbank enthalten ist.

Formatieren von Domainnamen in Lightsail

Um Benutzern den Zugriff auf die Website oder Anwendung zu erleichtern, wählen Sie einen Domänennamen, den man sich leicht merken kann. Domänennamen (und die Namen von DNS-Zonen und Datensätzen) bestehen aus einer Reihe von Bezeichnern, die durch Punkte (.) voneinander getrennt sind. Die Namenskonventionen hängen davon ab, ob Sie einen Domänennamen registrieren oder den Namen einer DNS-Zone oder eines Datensatzes angeben.

Formatieren Sie Ihren Domänennamen gemäß den folgenden Richtlinien.

Inhalt

Format der Domainnamen für die Domainnamenregistrierung

Für die Domänennamenregistrierung muss Ihr Domänenname 1–255 Zeichen lang sein. Zu den zulässigen Zeichen für Domänennamen gehören (a-z), (A-Z), (0-9), Bindestriche (-) und Punkte (.).

Sie können keine Leerzeichen verwenden oder einen Bindestrich am Anfang oder Ende eines Domainnamens setzen. Lightsail unterstützt jeden gültigen generischen Top-Level-Domainnamen (TLD). Weitere Informationen finden Sie unter Geografische Top-Level-Domains im Entwicklerhandbuch für Amazon Route 53.

Format der Domainnamen für DNS-Zonen und Datensätze

Für DNS-Zonen und -Datensätze muss der Domänenname 1–255 Zeichen lang sein. Zu den zulässigen Zeichen für Domänennamen gehören (a-z), (A-Z), (0-9), Bindestriche (-) und Punkte (.). Sie können keine Leerzeichen verwenden.

Lightsail speichert Buchstaben als Kleinbuchstaben (a-z), auch wenn Sie sie als Großbuchstaben (A-Z) angeben.

Lightsail unterstützt DNS-Zonen sowohl für generische als auch für geografische TLDs. Weitere Beispiele für geografische TLDs finden Sie unter Geografische Top-Level-Domains im Entwicklerhandbuch für Amazon Route 53..

Verwendung eines Sternchens (*) im Namen von DNS-Zonen und Datensätzen

Abhängig von seiner Position im Namen wird das Sternchen (*) vom DNS als Platzhalter behandelt. Ein Platzhalter-DNS-Datensatz ist ein Datensatz, der DNS-Anfragen für jede Subdomäne beantwortet, die Sie noch nicht definiert haben. In Lightsail können Sie unter den folgenden Bedingungen DNS-Zonen und -Datensätze erstellen, die das Sternchen (*) im Namen enthalten:

DNS-Zonen

- Ein Sternchen (*) kann nicht im Bezeichner ganz links in einem Domainnamen verwendet werden. Beispielsweise können Sie nicht subdomäne.*.beispiel.de verwenden.

- Wenn Sie ein Sternchen (*) in anderen Positionen verwenden, wird es von DNS wie ein ASCII-42-Zeichen und nicht als Platzhalter behandelt. Weitere Informationen zu ASCII-Zeichen finden Sie unter ASCII in der Wikipedia.

DNS-Datensätze

Bitte beachten Sie die folgenden Einschränkungen bei der Verwendung eines Sternchens (*) als Platzhalter im Namen eines DNS-Datensatzes:

- Als Platzhalter muss das Sternchen den Bezeichner ganz links in einem Domänennamen ersetzen, z. B. *.beispiel.de oder *.acme.example.com. Wenn Sie ein Sternchen in anderen Positionen verwenden (z. B. prod.*.example.com), wird es von DNS wie ein ASCII-42-Zeichen und nicht als Platzhalter behandelt.
- Das Sternchen muss den gesamten Bezeichner ersetzen. Sie können z. B. nicht *prod.beispiel.de oder prod*.beispiel.de angeben.
- Spezifische Domänennamen haben Vorrang. Wenn Sie zum Beispiel Datensätze für *.example.com und acme.example.com erstellen, werden DNS-Abfragen für acme.example.com immer mit den Werten im Datensatz acme.example.com beantwortet.
- Das Sternchen gilt für DNS-Abfragen für die Subdomäneneben, die das Sternchen enthält, und alle Subdomänen dieser Subdomäne. Wenn Sie beispielsweise einen Datensatz mit dem Namen *.example.com erstellen, werden DNS-Abfragen für *.example.com auf Folgendes antworten:

  zenith.example.com

  acme.zenith.example.com

  pinnacle.acme.zenith.example.com (falls es keine Einträge irgendwelcher Art für diese DNS-Zone gibt)

Wenn Sie einen Datensatz mit dem Namen *.example.com erstellen und es keinen Datensatz example.com gibt, antwortet Lightsail auf DNS-Abfragen für example.com mit `NXDOMAIN` (nicht existierende Domäne).

Sie können Lightsail so konfigurieren, dass es die gleiche Antwort auf DNS-Abfragen für alle Subdomänen auf derselben Ebene und auch für den Domänennamen zurückgibt. Beispielsweise können Sie Lightsail so konfigurieren, dass DNS-Abfragen wie acme.example.com und zenith.example.com unter Verwendung des Datensatzes example.com beantwortet werden. Führen

Sie die folgenden Schritte aus, um den Datenverkehr für Unterdomänen an die Top-Level-Domäne example.com weiterzuleiten:

1. Erstellen Sie einen Datensatz für die Domäne, wie z. B. example.com.
2. Erstellen Sie einen Alias-Datensatz für die Subdomäne, wie z. B. *.example.com. Geben Sie den Datensatz, den Sie im vorherigen Schritt erstellt haben, als Ziel für den Alias-Datensatz ein.

Nächste Schritte

Weitere Informationen finden Sie unter den folgenden Themen:

- Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain
- DNS

Eine Lightsail-Domain in Amazon Route 53 verwalten

Amazon Lightsail registriert Domains über Amazon Route 53, einen hochverfügbaren und skalierbaren DNS-Webservice. Wenn Sie eine Domain mit Lightsail registrieren, können Sie die Domain sowohl in Lightsail, als auch in Route 53 verwalten.

Aufgaben wie die Registrierung einer Domäne und die Weiterleitung des Datenverkehrs für eine Domäne an Lightsail-Ressourcen werden in der Lightsail-Konsole erledigt. Weitere Informationen finden Sie unter Domainregistrierung in Amazon Lightsail.

Erweiterte Aufgaben, wie das Übertragen von Domains und das Löschen Ihrer Registrierung, müssen in der Amazon-Route-53-Konsole durchgeführt werden.

Dieses Handbuch enthält Informationen zu einigen der erweiterten Verwaltungsaufgaben, die Sie mit der Route-53-Konsole ausführen können. Einen vollständigen Überblick über Route 53 finden Sie unter Was ist Amazon Route 53? im Entwicklerhandbuch für Amazon Route 53.

Inhalt

- Übertragen von Domains
- Löschen einer Domainnamen-Registrierung

Anzeigen des Status einer Domainregistrierung

Domänennamen haben einen Status, der auch als EPP-Statuscode (Extensible Provisioning Protocol) bezeichnet wird. ICANN, die Organisation, die eine zentrale Datenbank mit Domänennamen verwaltet, hat den EPP-Statuscode entwickelt. Die EPP-Statuscodes informieren Sie über den Status einer Vielzahl von Vorgängen, beispielsweise die Registrierung eines Domänennamens, die Verlängerung der Registrierung für einen Domänennamen usw. Alle Vergabestellen verwenden dieselben Statuscodes. Informationen zum Statuscode Ihrer Domains finden Sie unter Anzeigen des Status einer Domainregistrierung im Entwicklerhandbuch für Amazon Route 53.

Eine Domain sperren, um die nicht autorisierte Übertragung an eine andere Vergabestelle zu verhindern

Über die Domänenregistrierungen für alle generischen Top-Level-Domänen (TLDs) können Sie eine Domäne sperren, um zu verhindern, dass die Domäne ohne Ihre Zustimmung an eine andere Vergabestelle übertragen wird. Weitere Informationen finden Sie unter Sperren einer Domain zum Verhindern der nicht autorisierten Übertragung an eine andere Vergabestelle im Entwicklerhandbuch für Amazon Route 53.

Wiederherstellen einer abgelaufenen oder gelöschten Domain

Wenn Sie eine Domäne nicht vor dem Ende des Zeitraums für späte Verlängerung verlängern oder die Domäne versehentlich löschen, erlauben einige Registrierungsdatenbanken für Top-Level-Domänen (TLDs) die Wiederherstellung der Domäne, bevor sie von Dritten registriert werden kann. Verwenden Sie das verknüpfte Verfahren, um zu versuchen, Ihre Domänenregistrierung wiederherzustellen. Weitere Informationen finden Sie unter Wiederherstellen einer abgelaufenen oder gelöschten Domain im Entwicklerhandbuch für Amazon Route 53.

Übertragen von Domainregistrierungen

Sie können die Domainregistrierung von einer anderen Vergabestelle an Route 53 übertragen, von einem AWS-Konto zu einem anderen oder von Route 53 zu einer anderen Vergabestelle. Weitere Informationen finden Sie unter Übertragen von Domains im Entwicklerhandbuch für Amazon Route 53.

Löschen einer Domainnamen-Registrierung

Für die meisten Domänen oberster Ebene (Top-Level-Domains, TLDs) können Sie die Registrierung löschen, wenn Sie sie nicht mehr benötigen. Wenn die Registrierungsstelle das Löschen der Registrierung zulässt, führen Sie die Schritte in diesem Thema aus. Weitere Informationen finden Sie unter Löschen einer Domainnamenregistrierung im Amazon-Route 53-Entwicklerhandbuch.

Bereitstellen von Domaininformationen bei der Registrierung oder Übertragung einer Domain in Lightsail

Wenn Sie eine Domäne mit Amazon Lightsail registrieren, geben Sie Domäneninformationen wie den Registrierungszeitraum (Laufzeit) und Kontaktinformationen der Domäne an. Sie konfigurieren auch die automatische Domänenverlängerung und den Datenschutz.

Sie können auch Informationen für eine Domäne ändern, die derzeit in Lightsail registriert ist. Beachten Sie Folgendes:

- Wenn Sie die Kontaktinformationen für eine Domäne ändern, senden wir eine E-Mail-Benachrichtigung über die Änderung an den Registrierenden. Diese E-Mail stammt von noreply@amazon.com. Für die meisten Änderungen ist es nicht erforderlich, dass der Registrierende antwortet.
- Für Änderungen an Kontaktinformationen, die auch eine Änderung des Eigentümers bedeuten, senden wir dem Registrierenden eine zusätzliche E-Mail. ICANN, die Organisation, die eine zentrale Datenbank mit Domänennamen verwaltet, verlangt, dass der Registrierende-Kontakt den Empfang der E-Mail bestätigt. Weitere Informationen finden Sie unter Vorname, Nachname und Organisation weiter unten in diesem Abschnitt.

Weitere Informationen zum Ändern von Kontaktinformationen für eine bestehende Domain finden Sie unter Aktualisieren der Kontaktinformationen für eine Domain.

Von Ihnen angegebene Domänenformationen

- Laufzeit
- Automatische Domänenverlängerung
- Registrierenden-Kontakt sowie administrativer und technischer Kontakt
- Identisch mit dem Registrierenden

- Kontakttyp
- Vorname, Nachname
- Organisation
- E-Mail
- Telefon
- Adresse 1
- Adresse 2
- Land
- Status
- Ort
- Postleitzahl
- Datenschutz

Begriff

Der Registrierungszeitraum für die Domäne. Die Laufzeit beträgt in der Regel ein Jahr. Sie können die Laufzeit bei der Registrierung der Domäne aber auf bis zu zehn Jahre verlängern.

Automatische Domänenverlängerung

Wenn Sie eine Domäne mit Lightsail registrieren, wird die Domäne mit automatischer Verlängerung konfiguriert. Der automatische Verlängerungszeitraum beträgt in der Regel ein Jahr. Sie können auswählen, ob Lightsail die Domäne vor dem Ablauf automatisch verlängern soll. Die Registrierungsgebühr wird Ihrem AWS-Konto in Rechnung gestellt. Weitere Informationen finden Sie unter Domainregistrierungserneuerung.

> **Important**
>
> Wenn Sie die automatische Domänenverlängerung deaktivieren, wird die Registrierung für die Domäne nicht verlängert, wenn das Ablaufdatum verstrichen ist. Deshalb ist es möglich, dass Sie die Kontrolle über den Domänennamen verlieren.

Registrierenden-Kontakt sowie administrativer und technischer Kontakt

Standardmäßig verwenden wir die gleichen Informationen für alle drei Kontakte. Wenn Sie andere Informationen für einen oder mehrere Kontakte eingeben möchten, deaktivieren Sie das Kontrollkästchen neben Same as registrant (Identisch mit dem Registrierenden) für jeden Kontakt.

Identisch mit dem Registrierenden

Gibt an, ob die gleichen Kontaktinformationen für den Registrierenden der Domänen, den administrativen und den technischen Kontakt verwendet werden sollen.

Kontakttyp

Kategorie für diesen Kontakt. Beachten Sie Folgendes:

- Wenn Sie die Option Company (Unternehmen) oder Association (Vereinigung) wählen, müssen Sie einen Organisationsnamen eingeben.
- Bei einigen Top-Level-Domänen (TLDs) hängt die Verfügbarkeit des Datenschutzes vom ausgewählten Contact Type (Kontakttyp) ab. Informationen zu den Datenschutzeinstellungen für Ihre TLD finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können
-

Vorname, Nachname

Vor- und Nachname des Kontakts. Wir empfehlen für First Name (Vorname) und Last Name (Nachname) den Namen so einzugeben, wie er in Ihrem offiziellen Ausweis lautet. Für einige Änderungen an den Domäneneinstellungen müssen Sie einen Identitätsnachweis vorlegen. In diesen Fällen muss der Name in Ihrem Ausweis genau mit dem Namen des aktuellen Registrierenden-Kontakts der Domäne übereinstimmen.

Wenn Sie die E-Mail-Adresse für den Registrierenden-Kontakt ändern, senden wir diese E-Mail sowohl an die bisherige als auch die neue E-Mail-Adresse.

Organisation

Die Organisation, die dem Kontakt zugeordnet ist (falls zutreffend). Für den Registrierenden und administrative Kontakte ist dies in der Regel die Organisation, welche die Domäne registriert. Für den technischen Kontakt kann dies die Organisation sein, welche die Domäne verwaltet.

Wenn der Kontakttyp ein anderer Wert als Person ist und Sie das Feld Organization (Organisation) für den Registrierenden ändern, ändern Sie damit den Domänenbesitzer. ICANN verlangt, dass der Registrierende zur Bestätigung per E-Mail kontaktiert wird. Die E-Mail kommt von einer der folgenden E-Mail-Adressen:

- noreply@registrar.amazon.com – Für TLDs, die von der Amazon-Vergabestelle registriert wurden
- noreply@domainnameverification.net – Für TLDs, die von unserem Registrierungspartner Gandi registriert wurden

Unter Domains, die Sie mit Amazon Route 53 registrieren können sehen Sie, wer die Vergabestelle für die TLD ist.

Wenn Sie die E-Mail-Adresse für den Registrierenden-Kontakt ändern, senden wir diese E-Mail sowohl an die bisherige als auch die neue E-Mail-Adresse.

E-Mail

Die E-Mail-Adresse des Kontakts. Beachten Sie Folgendes:

Wenn Sie die E-Mail-Adresse für den Registrierenden-Kontakt ändern, senden wir Benachrichtigungs-E-Mails sowohl an die bisherige als auch die neue E-Mail-Adresse. Diese E-Mail stammt von noreply@amazon.com.

Telefon

Die Telefonnummer des Kontakts:

- Wenn Sie eine Telefonnummer für Standorte in den USA und Kanada eingeben, geben Sie 1 gefolgt von der 10-stelligen Telefonnummer mit Vorwahl ein.
- Wenn Sie eine Telefonnummer für einen anderen Standort eingeben, geben Sie den Ländercode gefolgt vom Rest der Telefonnummer ein. Eine Liste der internationalen Telefonnummern finden Sie in der Liste der internationalen Vorwahlnummern in der Wikipedia.

Adresse 1

Die Anschrift oder das Postfach für den Kontakt.

Adresse 2

Zusätzliche Adressinformationen für den Kontakt, z. B. Wohnung, Suite, Einheit, Gebäude, Etage oder Poststation.

Land

Das Land des Kontakts.

Status

Das Bundesland des Kontakts, sofern vorhanden.

Ort

Der Wohnort des Kontakts.

Postleitzahl

Die Postleitzahl des Kontakts.

Datenschutz

Wählen Sie, ob Sie Ihre Kontaktinformationen vor WHOIS-Abfragen verbergen möchten. Wenn Sie den Datenschutz für die Kontaktinformationen Ihrer Domäne aktivieren, werden bei WHOIS-Anfragen („who is“) anstelle Ihrer persönlichen Daten die Kontaktinformationen der Domänenvergabestelle zurückgegeben. Die Domänenvergabestelle ist das Unternehmen, das die Registrierung von Domänennamen verwaltet.

> **Note**
>
> Dieselbe Datenschutzeinstellung gilt für den Registrierenden-Kontakt sowie den administrativen und technischen Kontakt.

Wenn Sie den Datenschutz für die Kontaktinformationen Ihrer Domäne deaktivieren, erhalten Sie mehr E-Mail-Spam an die von Ihnen angegebene E-Mail-Adresse.

Jeder kann eine WHOIS-Abfrage für eine Domäne senden und erhält alle Kontaktinformationen für diese Domäne. Der WHOIS-Befehl ist in vielen Betriebssystemen verfügbar und steht zudem als Webanwendung auf vielen Webseiten zur Verfügung.

> **Important**
>
> Obwohl es berechtigte Benutzer für die Kontaktinformationen Ihrer Domäne gibt, sind es meist Spammer, die unerwünschte E-Mail- und Spam-Angebote an Domänenkontakte senden. Generell empfehlen wir, den Privacy Protection (Datenschutz) für Contact information (Kontaktinformationen) aktiviert zu lassen.

Weitere Informationen zum Datenschutz finden Sie in den folgenden Themen:

- Datenschutz für eine Domain verwalten
- Domains, die Sie mit Amazon Route 53 registrieren können

Verwalten der Erneuerung der Domainregistrierung in Lightsail

Wenn Sie eine Domäne mit Amazon Lightsail registrieren, wird die Domäne mit automatischer Verlängerung konfiguriert. Der automatische Verlängerungszeitraum beträgt standardmäßig ein Jahr, wobei einige Top-Level-Domänen (TLDs) längere Verlängerungszeiträume haben. Alle allgemeinen TLDs ermöglichen das Verlängern der Domänenregistrierung für längere Zeiträume, in der Regel bis zu zehn Jahren in Ein-Jahres-Schritten.

> **Note**
>
> Stellen Sie sicher, dass Sie die automatische Verlängerung deaktivieren, wenn Sie beabsichtigen, Ihr AWS-Konto zu schließen. Andernfalls wird Ihre Domänenregistrierung auch dann verlängert, nachdem Sie Ihr Konto geschlossen haben.

Inhalt

Automatische Verlängerung

Die folgende Zeitleiste zeigt, was geschieht, wenn die automatische Verlängerung aktiv ist:

45 Tage vor Ablauf

Wir senden eine E-Mail an den Registrierenden-Kontakt, um Ihnen mitzuteilen, dass die automatische Verlängerung aktiv ist. Die E-Mail enthält auch Anweisungen zur Deaktivierung der automatischen Verlängerung. Halten Sie die E-Mail-Adresse des Registrierenden-Kontakts aktuell, damit Sie diese E-Mail nicht verpassen.

35 oder 30 Tage vor Ablauf

Für alle Domänen außer .com.ar, .com.br und .jp verlängern wir die Domänenregistrierung 35 Tage vor dem Ablaufdatum. So haben wir Zeit, alle Probleme mit der Verlängerung zu lösen, bevor der Domänenname abläuft.

Die Registrierungen für die Domänen .com.ar, .com.br und .jp erfordern, dass wir die Domänen frühestens 30 Tage vor dem Ablaufdatum verlängern. Gandi, unsere Partner-Vergabestelle, sendet 30 Tage vor Ablauf eine Verlängerungs-E-Mail. Wenn die automatische Verlängerung aktiv ist, wird diese E-Mail am selben Tag gesendet, an dem wir die Domäne verlängern.

Wenn die automatische Verlängerung inaktiv ist, zeigt die folgende Zeitleiste, was passiert, wenn sich das Ablaufdatum des Domänennamens nähert:

45 Tage vor Ablauf

Wir senden eine E-Mail, um den Registrierenden-Kontakt darüber zu informieren, dass die automatische Verlängerung derzeit inaktiv ist. Die E-Mail enthält auch Anweisungen zur Aktivierung der automatischen Verlängerung. Halten Sie die E-Mail-Adresse des Registrierenden-Kontakts aktuell, damit Sie diese E-Mail nicht verpassen.

35 Tage und 7 Tage vor dem Ablauf

Wenn die automatische Verlängerung für die Domäne inaktiv ist, verlangt ICANN (das Verwaltungsorgan für die Domänenregistrierung), dass die Vergabestelle dem Registrierenden-Kontakt eine E-Mail sendet. Die E-Mail kommt von einer der folgenden E-Mail-Adressen:

noreply@registrar.amazon.com – Für Domains, deren Vergabestelle Amazon Registrar ist

noreply@domainnameverification.net – Für Domains, deren Vergabestelle unsere Partner-Vergabestelle Gandi ist

Wenn Sie die automatische Verlängerung weniger als 30 Tage vor Ablauf aktivieren, verlängern wir die Domänenregistrierung innerhalb von 24 Stunden.

Weitere Informationen zu Verlängerungszeiträumen finden Sie im Abschnitt "Fristen für die Verlängerung und Wiederherstellung von Domains" für Ihre TLD in Domains, die Sie mit Amazon Route 53 registrieren können im Entwicklerhandbuch für Amazon Route 53.

Nach dem Ablaufdatum

Die meisten Domänen werden von der Vergabestelle für eine kurze Zeit nach Ablauf beibehalten, sodass Sie möglicherweise eine abgelaufene Domäne nach dem Ablaufdatum noch verlängern können. Wir empfehlen jedoch, die automatische Verlängerung aktiv zu lassen, wenn Sie die Domäne behalten möchten. Weitere Informationen über die Verlängerung einer Domain nach dem Ablaufdatum finden Sie unter Wiederherstellen einer abgelaufenen oder gelöschten Domain im Entwicklerhandbuch für Amazon Route 53.

Wenn eine Domäne abläuft, für die Domäne aber eine späte Verlängerung zulässig ist, können Sie die Domäne zum Standardverlängerungspreis verlängern. Um zu ermitteln, ob sich eine Domain noch im Zeitraum für späte Verlängerung befindet, führen Sie die Schritte unter Verlängern des Registrierungszeitraums für eine Domain im Entwicklerhandbuch für Amazon Route 53 aus. Wenn die Domäne noch aufgelistet ist, befindet sie sich im Zeitraum für späte Verlängerung.

Automatische Verlängerung für eine Domäne bei der Domänenregistrierung konfigurieren

Wenn Sie einen neuen Domänennamen mit Lightsail registrieren, wird die Domäne mit automatischer Verlängerung konfiguriert. Sie können während der Domänenregistrierung wählen, ob Sie die automatische Domänenverlängerung deaktivieren möchten.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie die Registerkarte Domains & DNS (Domänen und DNS).
3. Wählen Sie die Schaltfläche Register domain (Domäne registrieren).
4. Geben Sie den Domainnamen an, den Sie mit Lightsail registrieren möchten, und wählen Sie dann Verfügbarkeit prüfen aus.
5. Wenn der Domänenname verfügbar ist, wird die Seite zur Domänenregistrierung angezeigt. Schalten Sie im Abschnitt Automatic domain renewal (Automatische Domänenverlängerung) die Umschalttaste ein oder aus, um die automatische Domänenverlängerung zu aktivieren oder zu deaktivieren.

Automatische Verlängerung für eine bereits registrierte Domäne konfigurieren

Wenn Sie die Einstellung ändern möchten, ob Lightsail die Registrierung für eine Domäne kurz vor dem Ablaufdatum automatisch verlängert, oder die aktuelle Einstellung für die automatische Verlängerung sehen möchten, führen Sie die folgenden Schritte durch.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie die Registerkarte Domains & DNS (Domänen und DNS).
3. Klicken Sie die Domäne, die Sie anzeigen oder aktualisieren möchten.
4. Wählen Sie die Registerkarte Contact info (Kontaktinformationen).
5. 5. Schalten Sie im Abschnitt Automatic domain renewal (Automatische Domänenverlängerung) die Umschalttaste ein oder aus, um die automatische Verlängerung für den Registrierungszeitraum der Domäne zu aktivieren oder zu deaktivieren.

Verwalten des Datenschutzes für Domainkontakte in Lightsail

Wenn Sie eine Domäne mit Lightsail registrieren, aktivieren wir den Datenschutz standardmäßig für alle Domänenkontakte. Dies blendet in der Regel die meisten Ihrer Kontaktinformationen aus WHOIS-Abfragen ("Wer ist wer?") aus und reduziert die Menge der Spam-Nachrichten, die Sie erhalten. Ihre Kontaktinformationen werden entweder durch Kontaktinformationen für die Vergabestelle oder durch die Bezeichnung "REDACTED FOR PRIVACY" (Für den Datenschutz unkenntlich gemacht) ersetzt. Für die Verwendung des Datenschutzes werden keine Gebühren erhoben.

Wenn Sie den Datenschutz deaktivieren, kann jeder eine WHOIS-Anfrage für die Domäne senden. Bei den meisten Top-Level-Domänen (TLDs) können so möglicherweise alle Kontaktinformationen abgerufen werden, die Sie bei der Registrierung der Domäne angegeben haben. Zu diesen Informationen gehören Name, Adresse, Telefonnummer und E-Mail-Adresse. Der WHOIS-Befehl ist weithin verfügbar. Er ist in vielen Betriebssystemen enthalten und steht zudem als Webanwendung auf vielen Webseiten zur Verfügung.

Um den Datenschutz für eine Domäne zu verwalten, die Sie mit Lightsail registriert haben, führen Sie die folgenden Schritte aus.

Inhalt

- Voraussetzungen erfüllen
- Datenschutz für Ihre Domäne verwalten

Erfüllen der Voraussetzungen

Registrieren Sie eine Domäne bei Lightsail. Weitere Informationen finden Sie unter Registrieren einer neuen Domain.

Datenschutz für Ihre Domäne verwalten

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie die Registerkarte Domains & DNS (Domänen und DNS).
3. Wählen Sie den Namen der Domäne aus, deren Datenschutz Sie ändern möchten.
4. Wählen Sie Contact info (Kontaktinformationen) aus.
5. Sie können den Datenschutz für Ihre Kontaktinformationen verwalten, indem Sie den Schalter Privacy protection (Datenschutz) ein- oder ausschalten.

Aktualisierung der Kontaktinformationen für eine Domain in Lightsail

Wenn Sie eine Domäne bei Amazon Lightsail registrieren, geben Sie Kontaktinformationen für Ihre Domäne an. Es gibt drei Arten von Kontaktinformationen:

- Registrierender: Besitzer der Domäne
- Administrativer Kontakt: Person, die für die Verwaltung Ihrer Domäne verantwortlich ist
- Technischer Kontakt: Person, die für technische Änderungen an Ihrer Domäne verantwortlich ist

Die Kontaktinformationen Ihrer Domäne werden verwendet, um die Eigentümerschaft Ihrer Domäne zu überprüfen und Sie über alle Informationen zu Ihrem Domänennamen auf dem Laufenden zu halten.

Topics

- Wer ist der Eigentümer einer Domäne?
- Aktualisierung der Kontaktinformationen für eine Domain

Wer ist der Eigentümer einer Domäne?

Wenn der Kontakttyp Person ist und Sie die Felder First Name oder Last Name für den Registrierenden ändern, ändern Sie damit den Eigentümer der Domäne.

Wenn der Kontakttyp ein andere Wert als Person ist und Sie Organization ändern, ändern Sie damit den Eigentümer der Domäne.

Die folgenden Aktionen werden ausgeführt, wenn Sie die Kontaktinformationen für eine Domäne ändern, die derzeit bei Lightsail registriert ist:

- Wenn Sie die Kontaktinformationen für eine Domäne ändern, senden wir eine E-Mail-Benachrichtigung über die Änderung an den Registrierenden. Diese E-Mail stammt von noreply@amazon.com. Für die meisten Änderungen ist es nicht erforderlich, dass der Registrierende antwortet.
- Für Änderungen an Kontaktinformationen, die auch eine Änderung des Eigentümers bedeuten, senden wir dem Registrierenden eine zusätzliche E-Mail. ICANN, die Organisation, die eine zentrale Datenbank mit Domänennamen verwaltet, verlangt, dass der Registrierenden-Kontakt den Empfang der E-Mail bestätigt.

Aktualisierung der Kontaktinformationen für eine Domain

Um die Kontaktinformationen für eine Domäne zu aktualisieren, führen Sie folgende Schritte durch.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie die Registerkarte Domains & DNS (Domänen und DNS).
3. Klicken Sie auf den Namen der Domäne, die Sie aktualisieren möchten.
4. Wählen Sie die Registerkarte Contact info (Kontaktinformationen). Wählen Sie dann Edit contact (Kontakt bearbeiten) aus.
5. Aktualisieren Sie die entsprechenden Werte. Weitere Informationen finden Sie unter Angegebene Werte beim Registrieren oder Übertragen einer Domain im Entwicklerhandbuch für Amazon Route 53.
6. Wählen Sie Save (Speichern).

Datenbanken in Amazon Lightsail

Sie können eine MySQL- oder PostgreSQL-verwaltete Datenbank in Amazon Lightsail in wenigen Schritten erstellen. Lightsail macht die Datenbankverwaltung effizienter, indem es Ihre gängigen Wartungs- und Sicherheitsaufgaben verwaltet. Mit der Lightsail-Konsole können Sie:

- Sichern Ihrer Datenbank in einem Snapshot
- Erstellen einer neuen, größere Datenbank aus einem Snapshot
- Beheben häufiger Probleme mit browserbasierten Protokollen und Metriken
- Stellen Sie Daten mithilfe von point-in-time Sicherungs- und Wiederherstellungsvorgängen wieder her.

Sie können Ihre Anwendung auf einer Lightsail-Instance erstellen und sie mit einer von Lightsail verwalteten Datenbank verbinden. Sie können außerdem eine eigenständige Datenbank erstellen und Analyse- oder Abfragetools Ihres Unternehmens verbinden. Wählen Sie aus Standard- oder Hochverfügbarkeitsdatenbankplänen, die Ihre vorkonfigurierte Datenbank, SSD-basierten Speicher und ein Datentransferkontingent zu einem festen, monatlichen Preis beinhalten. Sie können Lightsail-Datenbanken auch über die AWS Command Line Interface (AWS CLI), API oder das SDK verwalten.

Auswählen einer Lightsail-Datenbank

Amazon Lightsail bietet die neuesten Hauptversionen der MySQL- und PostgreSQL-Datenbanken. Diese Anleitung hilft Ihnen bei der Entscheidung, welche Datenbank für Ihr Projekt die richtige ist.

Lightsail bietet auch eine Windows Server 2022-Instance mit SQL Server an. Weitere Informationen finden Sie unter Auswählen eines Amazon Lightsail-Instance-Images.

Vergleich der verwalteten Datenbanken in Lightsail

MySQL

MySQL 5.7 und 8.0 sind in Lightsail verfügbar. MySQL ist die am weitesten verbreitete relationale Open-Source-Datenbank. Sie dient als primärer, relationaler Datenspeicher für viele beliebte Websites, Anwendungen und kommerzielle Produkte. MySQL ist ein zuverlässiges, stabiles und sicheres SQL-basiertes Datenbankmanagementsystem mit mehr als 20 Jahren Community-gestützter

Entwicklung und Support. Die MySQL-Datenbank eignet sich für eine Vielzahl von Anwendungsfällen, darunter geschäftskritische Anwendungen und dynamische Websites. Sie arbeitet außerdem als eingebettete Datenbank für Software, Hardware und Geräte.

> **Important**
>
> Ab dem 30. Juni 2024 unterstützt Lightsail MySQL 5.7 nicht mehr und Sie können mit diesem Blueprint keine neuen Datenbanken mehr erstellen. Informationen zum Aktualisieren von Hauptversionen Ihrer Datenbank-Instance finden Sie unter Aktualisieren der Hauptversion einer Lightsail-Datenbank.

Weitere Informationen finden Sie in der folgenden MySQL-Dokumentation:

- MySQL 5.7-Dokumentation
- MySQL 8.0-Dokumentation

PostgreSQL

PostgreSQL 11, 12, 13, 14, 15 und 16 sind in Lightsail verfügbar. PostgreSQL ist ein leistungsfähiges, objektrelationales Open-Source-Datenbanksystem mit mehr als 30 Jahren aktiver Entwicklung und einem sehr guten Ruf für tadellose Zuverlässigkeit, Feature, Robustheit und Leistung.

Es gibt eine Fülle an Informationen zur Installation und Verwendung von PostgreSQL im Rahmen der offiziellen Dokumentation. Die PostgreSQL-Community bietet viele Möglichkeiten, sich mit den Technologien vertraut zu machen, zu erfahren, wie sie funktioniert und Karrieremöglichkeiten zu finden.

> **Important**
>
> Ab dem 30. Juni 2024 unterstützt Lightsail PostgreSQL 11 nicht mehr und Sie können mit diesem Blueprint keine neuen Datenbanken mehr erstellen. Informationen zum Aktualisieren von Hauptversionen Ihrer Datenbank-Instance finden Sie unter Aktualisieren der Hauptversion einer Lightsail-Datenbank.

Weitere Informationen finden Sie in der folgenden PostgreSQL-Dokumentation:

- PostgreSQL-11-Dokumentation
- PostgreSQL-12-Dokumentation
- PostgreSQL 13-Dokumentation
- PostgreSQL 14-Dokumentation
- PostgreSQL 15-Dokumentation
- PostgreSQL 16-Dokumentation

Datenimport optimieren

In Lightsail sind mehrere Datenbankpläne verfügbar, die jeweils bestimmte Spezifikationen für Arbeitsspeicher, vCPU, Speicher und Datenübertragungszulage aufweisen. Da jeder Datenbankplan diese Spezifikationen hat, ist es wichtig, dass Sie einen Datenbankplan mit der entsprechenden Größe für die Datenmenge auswählen, die Sie in Ihre neue Lightsail-Datenbank importieren möchten. Ihr Datenimport kann verlangsamt werden, wenn Sie einen Plan auswählen, der unter Ihren Größenanforderungen liegt. Verwenden Sie die folgenden Richtlinien, um den geeigneten Datenbankplan für Ihre Datenimportanforderung auszuwählen:

- Micro-Datenbankblan (15 USD/Monat) - Der Datenimport kann bei Übertragungen von mehr als 10 GB verlangsamt sein.
- Small-Datenbankplan (30 USD /Monat) – Der Datenimport kann bei Übertragungen von mehr als 20 GB verlangsamt sein.
- Medium-Datenbankplan (60 USD/Monat) – Der Datenimport kann bei Übertragungen von mehr als 85 GB verlangsamt sein.
- Large-Datenbankplan (115 USD/Monat) – Der Datenimport kann bei Übertragungen von mehr als 156 GB verlangsamt sein.

> **Note**
>
> Weitere Informationen zum Importieren von Daten in Ihre Datenbank finden Sie unter Importieren von Daten in Ihre MySQL-Datenbank oder Importieren von Daten in Ihre PostgreSQL-Datenbank.

Hochverfügbarkeitsdatenbanken in Lightsail

Eine hochverfügbare verwaltete Datenbank in Lightsail bietet Failover-Unterstützung durch eine primäre Datenbank in einer Availability Zone und eine sekundäre Standby-Datenbank in einer anderen. Wir empfehlen Hochverfügbarkeitsdatenbanken für Produktions-Workloads, die stark ausgelastet sind und Datenredundanz erfordern. Für Entwicklungs- und Testzwecke können Sie eine Standarddatenbank verwenden, die nicht hochverfügbar ist.

Um eine Hochverfügbarkeitsdatenbank zu erstellen, wählen Sie beim Erstellen Ihrer verwalteten Datenbank einen der in Lightsail verfügbaren Hochverfügbarkeitsdatenbankpläne aus. Weitere Informationen finden Sie unter Erstellen einer Datenbank. Sie können Ihre Standarddatenbank auch in eine Hochverfügbarkeitsdatenbank umwandeln. Erstellen Sie einen Snapshot Ihrer Standarddatenbank, erstellen Sie eine neue Datenbank aus dem Snapshot und wählen Sie einen Hochverfügbarkeitsplan. Weitere Informationen finden Sie unter Erstellen einer Datenbank aus einem Snapshot.

Erstellen einer Lightsail-Datenbank

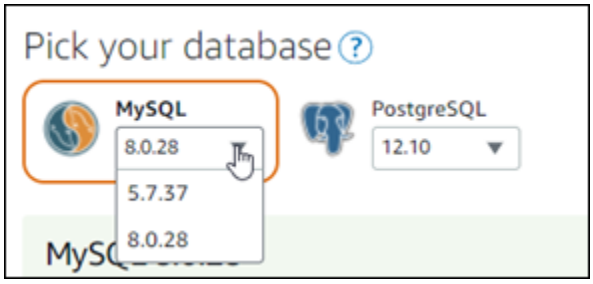
Erstellen Sie in wenigen Minuten eine verwaltete Datenbank in Amazon Lightsail. Sie können zwischen den beiden neuesten Major-Versionen von MySQL wählen und Ihre Datenbank mit einem Standard- oder Hochverfügbarkeitsplan konfigurieren.

> **Note**
>
> Weitere Informationen zu den verwalteten Datenbanken in Lightsail finden Sie unter Auswahl einer Datenbank.

Eine Datenbank erstellen

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Databases (Datenbanken) aus.
3. Wählen Sie Datenbank erstellen aus.
4. Wählen Sie die AWS-Region und Availability Zone für Ihre Datenbank aus.
    1. Wählen Sie AWS-Region und Availability Zone ändern aus und wählen Sie eine Region.
    2. Wählen Sie Change your Availability Zone (Ihre Availability Zone ändern) und wählen Sie dann eine Availability Zone aus.

5. Wählen Sie Ihren Datenbanktyp aus. Wählen Sie unter einer der verfügbaren Optionen für die Datenbank-Engine das Dropdownmenü und dann eine der neuesten von Lightsail unterstützten Major-Datenbankversionen.



6. Wählen Sie bei Bedarf eine dieser Optionen aus:

   - Specify login credentials (Anmeldedaten angeben) – Geben Sie Ihren eigenen Datenbankbenutzernamen und Ihr eigenes Passwort an. Andernfalls legt Lightsail den Benutzernamen fest und erstellt ein sicheres Passwort für Sie.
     - Um Ihren eigenen Benutzernamen anzugeben, wählen Sie Specify login credentials (Anmeldedaten angeben) aus und geben Sie Ihren Benutzernamen in das Textfeld ein. Die folgenden Einschränkungen gelten je nach Datenbank-Engine, die Sie auswählen:

       MySQL

       - Erforderlich für MySQL.
       - Muss 1 bis 16 Buchstaben oder Zahlen enthalten.
       - Muss mit einem Buchstaben beginnen.
       - Darf kein Wort sein, das für die ausgewählte Datenbank-Engine reserviert ist. Weitere Informationen zu reservierten Wörtern in MySQL finden Sie in den Artikeln „Schlüssel- und Reservierte Wörter“ fürMySQL 5.6,MySQL 5.7, oderMySQL 8.0.

       PostgreSQL

       - Erforderlich für PostgreSQL.
       - Muss 1 bis 63 Buchstaben oder Zahlen enthalten.
       - Muss mit einem Buchstaben beginnen.
       - Darf kein Wort sein, das für die ausgewählte Datenbank-Engine reserviert ist. Weitere Informationen über reservierte Wörter in PostgreSQL finden Sie in den SQL-Schlüsselwortartikeln für PostgreSQL 9.6, PostgreSQL 10, PostgreSQL 11 oder PostgreSQL 12.

- Um Ihr eigenes Passwort festzulegen, deaktivieren Sie das Kontrollkästchen Create a strong password for me (Ein starkes Passwort für mich erstellen) und geben Sie Ihr Passwort in das Textfeld ein. Das Passwort kann jedes druckbare ASCII-Zeichen mit Ausnahme von "/", """ oder "@" enthalten. Für MySQL-Datenbanken kann das Passwort zwischen 8 und 41 Zeichen enthalten. Für PostgreSQL-Datenbanken kann das Passwort zwischen 8 und 128 Zeichen enthalten.

- Specify the master database name (Namen der Hauptdatenbank festlegen) – Geben Sie Ihren eigenen primären Datenbanknamen an, oder Lightsail legt den Namen für Sie fest. Um Ihren eigenen primären Datenbanknamen anzugeben, wählen Sie Specify the master database name (Namen der Hauptdatenbank festlegen) und geben einen Namen in das Textfeld ein. Die folgenden Einschränkungen gelten je nach Datenbank-Engine, die Sie auswählen:

  MySQL

  - Muss 1 bis 64 Buchstaben oder Zahlen enthalten.
  - Er muss mit einem Buchstaben beginnen. Nachfolgende Zeichen können Groß-, Kleinbuchstaben oder Zahlen (0-9) sein.
  - Darf kein Wort sein, das für die ausgewählte Datenbank-Engine reserviert ist. Weitere Informationen zu reservierten Wörtern in MySQL finden Sie in den Artikeln „Schlüssel- und Reservierte Wörter“ fürMySQL 5.6,MySQL 5.7, oderMySQL 8.0.

  PostgreSQL

  - Muss 1 bis 63 Buchstaben, Zahlen oder Unterstriche enthalten.
  - Er muss mit einem Buchstaben beginnen. Nachfolgende Zeichen können Groß-, Kleinbuchstaben oder Zahlen (0-9) sein.
  - Darf kein Wort sein, das für die ausgewählte Datenbank-Engine reserviert ist. Weitere Informationen über reservierte Wörter in PostgreSQL finden Sie in den SQL-Schlüsselwortartikeln für PostgreSQL 9.6, PostgreSQL 10, PostgreSQL 11 oder PostgreSQL 12.

7. Wählen Sie einen Hochverfügbarkeits- oder einen Standard-Datenbankplan aus.

   Eine mit einem Hochverfügbarkeitsplan erstellte Datenbank verfügt über eine primäre Datenbank und eine sekundäre Standby-Datenbank in einer anderen Availability Zone für die Failover-Unterstützung. Weitere Informationen finden Sie unter Hochverfügbarkeitsdatenbanken.
   Es stehen verschiedene, preiswerte Datenbankpaket-Optionen zur Verfügung – jeweils mit unterschiedlichem Arbeitsspeicher-, Datenverarbeitungs-, Speicherplatz- und Übertragungsraten.

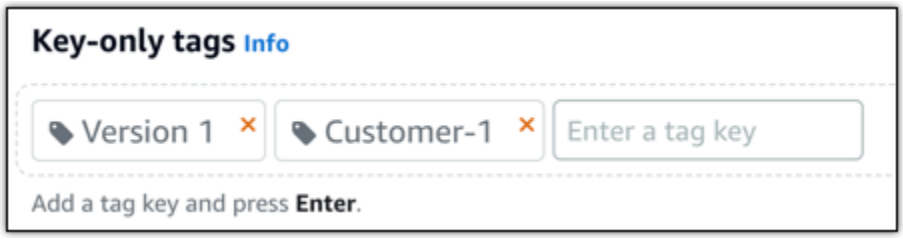
8. Geben Sie einen Namen für Ihre Datenbank ein.

   Ressourcennamen:

   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

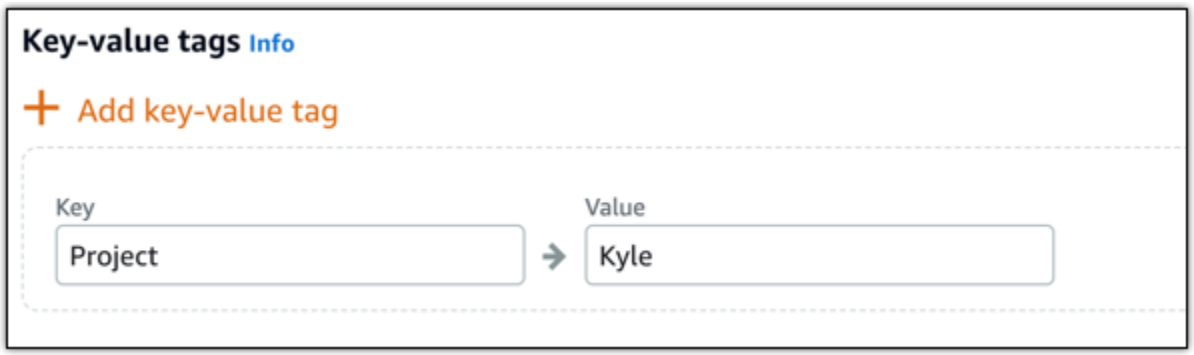
9. Wählen Sie eine der folgenden Optionen aus, um Ihrer Datenbank Tags hinzuzufügen:

   - Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.

   - Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

     Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.

> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

10. Wählen Sie Datenbank erstellen aus.

    Innerhalb weniger Minuten ist Ihre Lightsail-Datenbank bereit. Sie können mit der Konfiguration für den Datenimport beginnen oder sich über einen Datenbank-Client mit ihr verbinden.

Nächste Schritte

Hier sind ein paar Anleitungen, die Ihnen helfen sollen, Ihre neue Datenbank nach der Inbetriebnahme in Lightsail zu verwalten:

- Konfigurieren des Datenimportmodus für Ihre Datenbank
- Konfigurieren des öffentlichen Modus für Ihre Datenbank in Amazon Lightsail
- Verwalten Ihres Datenbankpassworts
- Verbinden mit Ihrer MySQL-Datenbank
- Herstellen einer Verbindung zu Ihrer PostgreSQL-Datenbank
- Importieren von Daten in Ihre MySQL-Datenbank
- Importieren von Daten in Ihre PostgreSQL-Datenbank
- Einen Snapshot Ihrer Datenbank erstellen

Verbinden mit Ihrer Lightsail-MySQL-Datenbank

Nachdem Ihre MySQL-verwaltete Datenbank in Amazon Lightsail erstellt wurde, können Sie jede standardmäßige MySQL-Clientanwendung oder ein Dienstprogramm verwenden, um sich mit ihr zu verbinden. Sie müssen den Datenbank-Endpunkt, den Port, den Benutzernamen und das Passwort von Ihrer Seite zur Datenbankverwaltung in der Lightsail-Konsole abrufen. Geben Sie diese Werte bei der Konfiguration der Datenbankverbindung in Ihrem Client oder Ihrer Webanwendung an.

Diese Anleitung zeigt Ihnen, wie Sie die erforderlichen Verbindungsinformationen erhalten und wie Sie MySQL Workbench so konfigurieren, dass es sich mit Ihrer verwalteten Datenbank verbindet.

> **Note**
>
> Weitere Informationen zum Herstellen einer Verbindung mit einer PostgreSQL-Datenbank finden Sie unter Herstellen einer Verbindung zu Ihrer PostgreSQL-Datenbank.

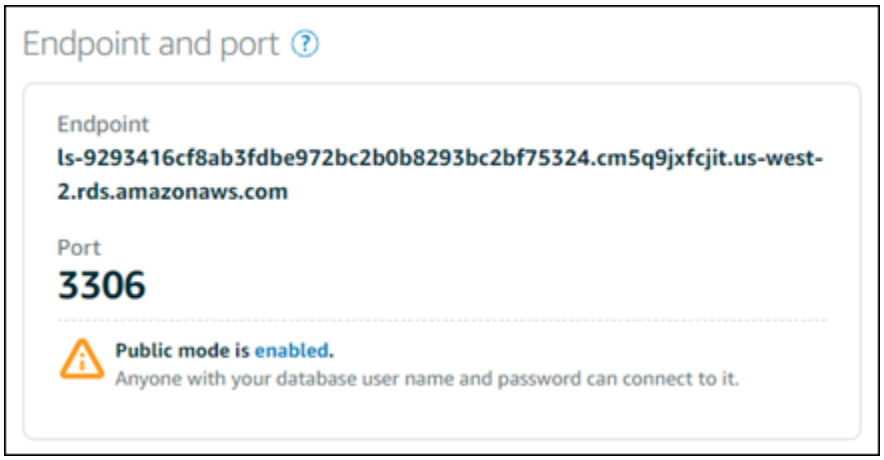
Schritt 1: Abrufen der Daten für Ihre MySQL-Datenbankverbindung

Holen Sie sich Ihre Datenbank-Endpunkt- und Port-Informationen aus der Lightsail-Konsole. Diese verwenden Sie später bei der Konfiguration Ihres Clients für die Verbindung mit Ihrer Datenbank.

So erhalten Sie Ihre Datenbankverbindungsdaten

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Databases (Datenbanken) aus.
3. Wählen Sie den Namen der Datenbank aus, mit der Sie sich verbinden möchten.
4. Notieren Sie sich auf der Registerkarte Connect (Verbinden) unter dem Abschnitt Endpoint and port (Endpunkt und Port) die Informationen zu Endpunkt und Port.

   Wir empfehlen, den Endpunkt in die Zwischenablage zu kopieren, um eine falsche Eingabe zu vermeiden. Markieren Sie dazu den Endpunkt und drücken Sie Ctrl+C (Strg+C), wenn Sie Windows verwenden, oder Cmd+C, wenn Sie MacOS verwenden, um ihn in die Zwischenablage zu kopieren. Drücken Sie dann Strg+V oder Cmd+V, um ihn einzufügen.

5. Klicken Sie auf der Registerkarte Connect (Verbinden) im Abschnitt User name and passwords (Benutzername und Passwörter), notieren Sie sich den Benutzernamen, und wählen Sie dann Show (Anzeigen) unter dem Abschnitt Password (Passwort), um das aktuelle Datenbankpasswort anzuzeigen.

Da verwaltete Passwörter komplex sind, empfehlen wir, sie zu kopieren und einzufügen, um eine falsche Eingabe zu vermeiden. Markieren Sie das verwaltete Passwort und drücken Sie Ctrl+C (Strg+C), wenn Sie Windows verwenden, oder Cmd+C, wenn Sie MacOS verwenden, um es in die Zwischenablage zu kopieren. Drücken Sie dann Strg+V oder Cmd+V, um ihn einzufügen.

Schritt 2: Konfigurieren der öffentlichen Verfügbarkeit Ihrer MySQL-Datenbank

Sie müssen den öffentlichen Modus aktivieren, damit sich Ihre Datenbank extern oder von einer Lightsail-Instance in einer anderen AWS-Region als Ihrer Datenbank mit ihr verbinden kann. Wenn der öffentliche Modus aktiviert ist, kann sich jeder mit dem Datenbankbenutzernamen und dem Passwort mit Ihrer Datenbank verbinden. Um die öffentliche Verfügbarkeit Ihrer Datenbank zu konfigurieren, befolgen Sie die Schritte im Handbuch Konfigurieren des öffentlichen Modus für Ihre Datenbank.

> **Note**
>
> Gehen Sie zu Schritt 3 über, wenn Sie eine Verbindung zu Ihrer Datenbank von einer Ihrer Lightsail-Instances aus planen, die sich in derselben Region wie Ihre Datenbank befindet.

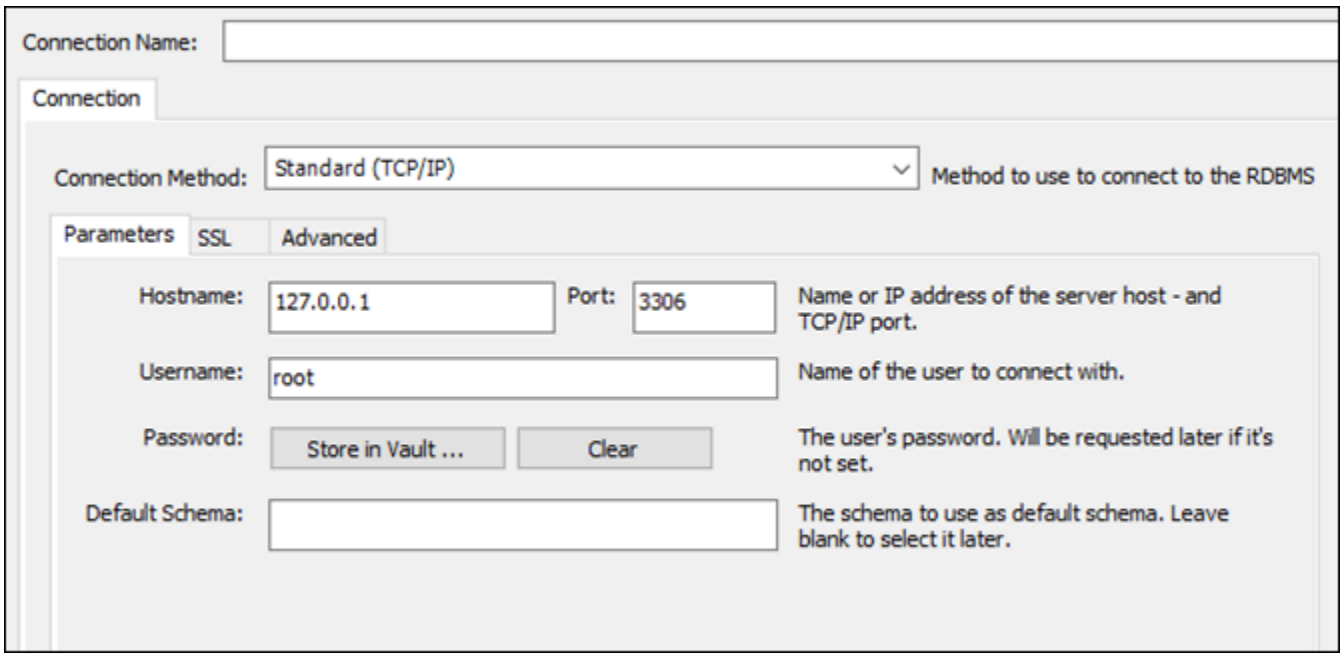
Schritt 3: Konfigurieren Ihres Datenbank-Clients für die Verbindung mit Ihrer MySQL-Datenbank

Um eine Verbindung zu Ihrer MySQL-Datenbank herzustellen, konfigurieren Sie Ihren Datenbank-Client so, dass er den Endpunkt und den Port verwendet, den Sie zuvor erhalten haben. Die folgenden Schritte veranschaulichen, wie Sie MySQL Workbench konfigurieren, diese Schritte sind aber möglicherweise sehr ähnlich mit denen für andere Clients.

> **Note**
>
> Weitere Informationen zur Verwendung von MySQL Workbench finden Sie im MySQL Workbench-Handbuch.

So konfigurieren Sie MySQL Workbench für die Verbindung zu Ihrer Datenbank:

1. Öffnen Sie MySQL Workbench.
2. Wählen Sie das Menü Database (Datenbank) und dann Manage connections (Verbindungen verwalten) aus.
3. Geben Sie die folgenden Informationen in das angezeigte Formular ein:



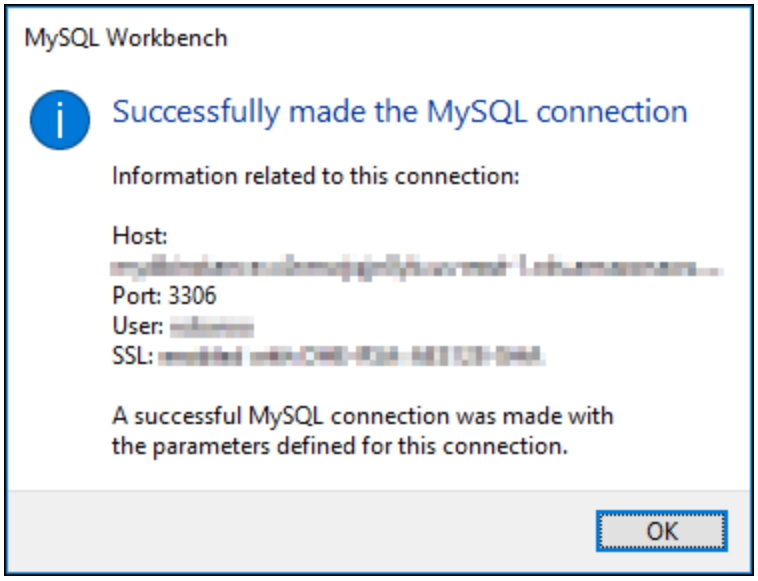
- Verbindungsname – Wir empfehlen, einen Namen für die Verbindung zu verwenden, der Ihrer Datenbank ähnlich ist. Dies hilft Ihnen, sie in Zukunft zu identifizieren.
- Connection Method (Verbindungsmethode) – Wählen Sie Standard (TCP/IP) aus.
- Port – Geben Sie den Port für Ihre Datenbank ein, den Sie zuvor erhalten haben. Der Standardport für MySQL ist 3306.
- Hostname – Geben Sie den Datenbank-Endpunkt ein, den Sie zuvor erhalten haben. Wenn Sie den Datenbank-Endpunkt aus der Lightsail-Konsole kopiert haben und er sich noch in der Zwischenablage befindet, drücken Sie Strg+V, wenn Sie Windows verwenden, oder Cmd+V, wenn Sie MacOS verwenden, um ihn einzufügen.
- Username (Benutzername) – Geben Sie den Datenbankbenutzernamen ein, den Sie zuvor erhalten haben.
- Passwort – Wählen Sie Store in vault (Speichern im Tresor) aus. Geben Sie in dem erscheinenden Fenster Ihr zuvor erhaltenes Datenbankpasswort ein. Wenn Sie das Passwort aus der Lightsail-Konsole kopiert haben und es sich noch in der Zwischenablage befindet,

drücken Sie Strg+V, wenn Sie Windows verwenden, oder Cmd+V, wenn Sie MacOS verwenden, um es einzufügen. Wählen Sie OK aus, um Ihr Passwort zu speichern.

- Standardschema – Lassen Sie dieses Textfeld leer.

4. Wählen Sie Test connection (Verbindung testen) aus, um festzustellen, ob der Client eine Verbindung zu Ihrer Datenbank herstellen kann.

   Wenn die Verbindung erfolgreich ist, erscheint eine Eingabeaufforderung ähnlich dem folgenden Beispiel. Nachdem Sie die Informationen gelesen haben, wählen Sie OK aus, um sie zu schließen.

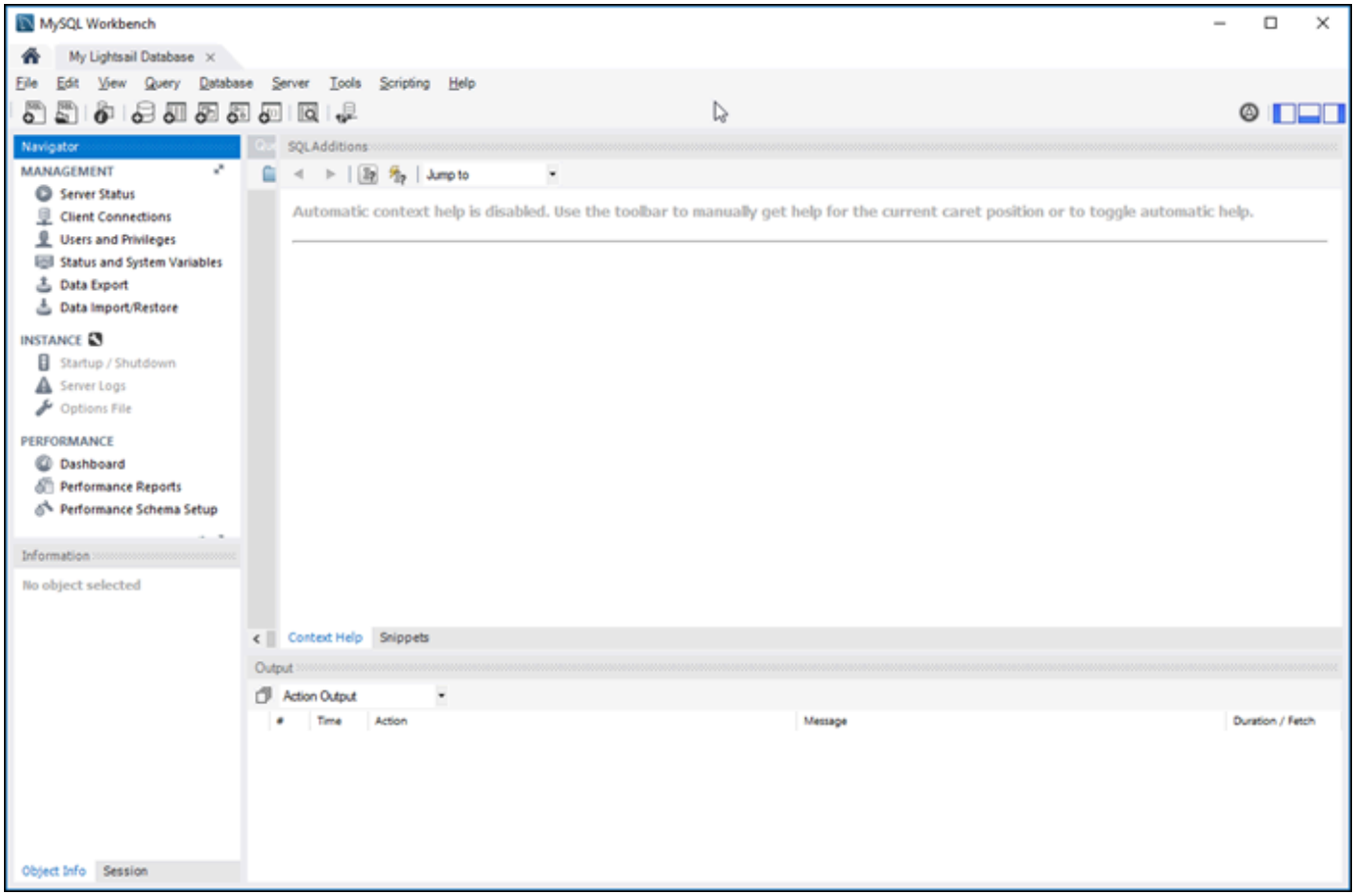


5. Wählen Sie New (Neu) aus, um die neuen Verbindungsdetails zu speichern, und wählen Sie dann Close (Schließen) aus, um das Fenster für die Verbindungsverwaltung zu schließen.

   Ihre neue Datenbankverbindung erscheint auf der Startseite der MySQL Workbench-Anwendung unter dem Abschnitt MySQL-Verbindungen.

6. Um eine Verbindung zu Ihrer Datenbank herzustellen, wählen Sie Ihre neue Datenbankverbindung aus.

   Wenn die Verbindung erfolgreich ist, erscheint ein Fenster ähnlich dem folgenden Beispiel.



Nächste Schritte

Hier ist eine Anleitung, die Ihnen hilft, Daten in Ihre Datenbank in Lightsail zu importieren:

- Importieren von Daten in Ihre MySQL-Datenbank

Verbinden mit Ihrer Lightsail-MySQL-Datenbank mithilfe von SSL

Amazon Lightsail erstellt ein SSL-Zertifikat und installiert es in Ihrer von MySQL verwalteten Datenbank, wenn es bereitgestellt wird. Das Zertifikat ist von einer Zertifizierungsstelle (Certificate Authority, CA) signiert und enthält den Datenbankendpunkt als Common Name (CN) für das SSL-Zertifikat, um vor Spoofing-Angriffen zu schützen.

Ein SSL-Zertifikat, das von Lightsail erstellt wurde, ist die vertrauenswürdige Root Entity und sollte in den meisten Fällen funktionieren, könnte jedoch fehlschlagen, wenn Ihre Anwendung keine

Zertifikatsketten akzeptiert. Wenn Ihre Anwendung keine Zertifikatsketten akzeptiert, müssen Sie evtl. ein Zwischenzertifikat verwenden, um sich mit Ihrer AWS-Region zu verbinden.

Weitere Informationen zu den CA-Zertifikaten für die verwaltete Datenbank, zu den unterstützten AWS-Regionen und zum Herunterladen von Zwischenzertifikaten für Ihre Anwendungen finden Sie unter Herunterladen eines SSL-Zertifikats für Ihre verwaltete Datenbank.

Unterstützte Verbindungen

MySQL verwendet yaSSL für sichere Verbindungen in folgenden Versionen:

- MySQL Version 5.7.19 und frühere 5.7-Versionen
- MySQL Version 5.6.37 und frühere 5.6-Versionen
- MySQL Version 5.5.57 und frühere 5.5-Versionen

MySQL verwendet OpenSSL für sichere Verbindungen in folgenden Versionen:

- MySQL-Version 8.0
- MySQL Version 5.7.21 und höhere 5.7-Versionen
- MySQL Version 5.6.39 und höhere 5.6-Versionen
- MySQL Version 5.5.59 und höhere 5.5-Versionen

MySQL-verwaltete Datenbanken unterstützen Transport Layer Security (TLS) Versionen 1.0, 1.1 und 1.2. Die folgende Liste zeigt die TLS-Unterstützung für MySQL-Versionen:

- MySQL 8.0 - TLS1.0, TLS 1.1 und TLS 1.2
- MySQL 5.7 - TLS1.0 und TLS 1.1. TLS 1.2 wird nur für MySQL 5.7.21 und höher unterstützt.
- MySQL 5.6 - TLS1.0
- MySQL 5.5 - TLS1.0

Voraussetzungen

- Installieren Sie MySQL Server auf dem Computer, mit dem Sie eine Verbindung zu Ihrer Datenbank herstellen. Weitere Informationen finden Sie unter MySQL Community Server-Download auf der MySQL-Website.

- Laden Sie das entsprechende Zertifikat für Ihre Datenbank herunter. Weitere Informationen finden Sie unter Herunterladen eines SSL-Zertifikats für die verwaltete Datenbank.

Verbinden mit Ihrer MySQL-Datenbank mithilfe von SSL

Führen Sie die folgenden Schritte aus, um eine Verbindung mit Ihrer MySQL-Datenbank mithilfe von SSL herzustellen.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie je nach Version Ihrer MySQL-Datenbank einen der folgenden Befehle ein:

   - Geben Sie den folgenden Befehl ein, um eine Verbindung mit einer Datenbank herzustellen, die MySQL 5.7 oder höher ist.

     ```
     mysql -h DatabaseEndpoint --ssl-ca=/path/to/certificate/rds-combined-ca-bundle.pem --ssl-mode=VERIFY_IDENTITY -u UserName -p
     ```

     Ersetzen Sie im Befehl Folgendes:

     - *DatabaseEndpoint* mit dem Endpunkt Ihrer Datenbank.
     - */path/to/certificate/rds-combined-ca-bundle.pem* mit dem lokalen Pfad, in dem Sie das Zertifikat für Ihre Datenbank heruntergeladen und gespeichert haben.
     - *UserName* mit dem Benutzernamen Ihrer Datenbank.

     Beispiel:

     ```
     mysql -h ls-1c51a7c70a4fb55e542829a4e4e0d735ba42.czowadgeezqi.us-west-2.rds.amazonaws.com --ssl-ca=/home/ec2-user/rds-combined-ca-bundle.pem --ssl-mode=VERIFY_IDENTITY -u dbmasteruser -p
     ```

   - Geben Sie den folgenden Befehl ein, um eine Verbindung mit einer Datenbank herzustellen, die MySQL 6.7 oder früher ist.

     ```
     mysql -h DatabaseEndpoint --ssl-ca=/path/to/certificate/rds-combined-ca-bundle.pem --ssl-verify-server-cert -u UserName -p
     ```

     Ersetzen Sie im Befehl Folgendes:

     - *DatabaseEndpoint* mit dem Endpunkt Ihrer Datenbank.

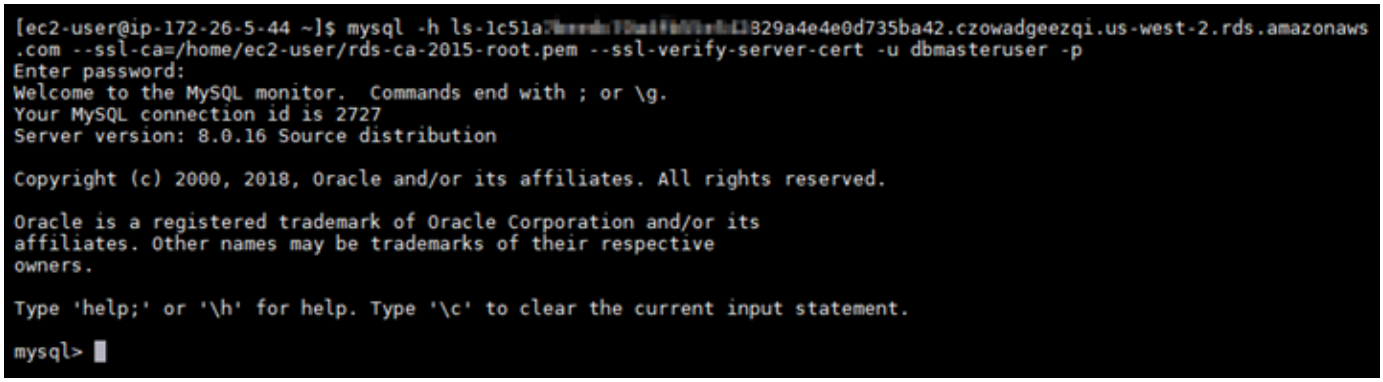
- */path/to/certificate/rds-combined-ca-bundle.pem* mit dem lokalen Pfad, in dem Sie das Zertifikat für Ihre Datenbank heruntergeladen und gespeichert haben.
- *UserName* mit dem Benutzernamen Ihrer Datenbank.

Beispiel:

```
mysql -h ls-1c51a7c70a4fb55e542829a4e4e0d735ba42.czowadgeezqi.us-
west-2.rds.amazonaws.com --ssl-ca=/home/ec2-user/rds-combined-ca-bundle.pem --
ssl-verify-server-cert -u dbmasteruser -p
```

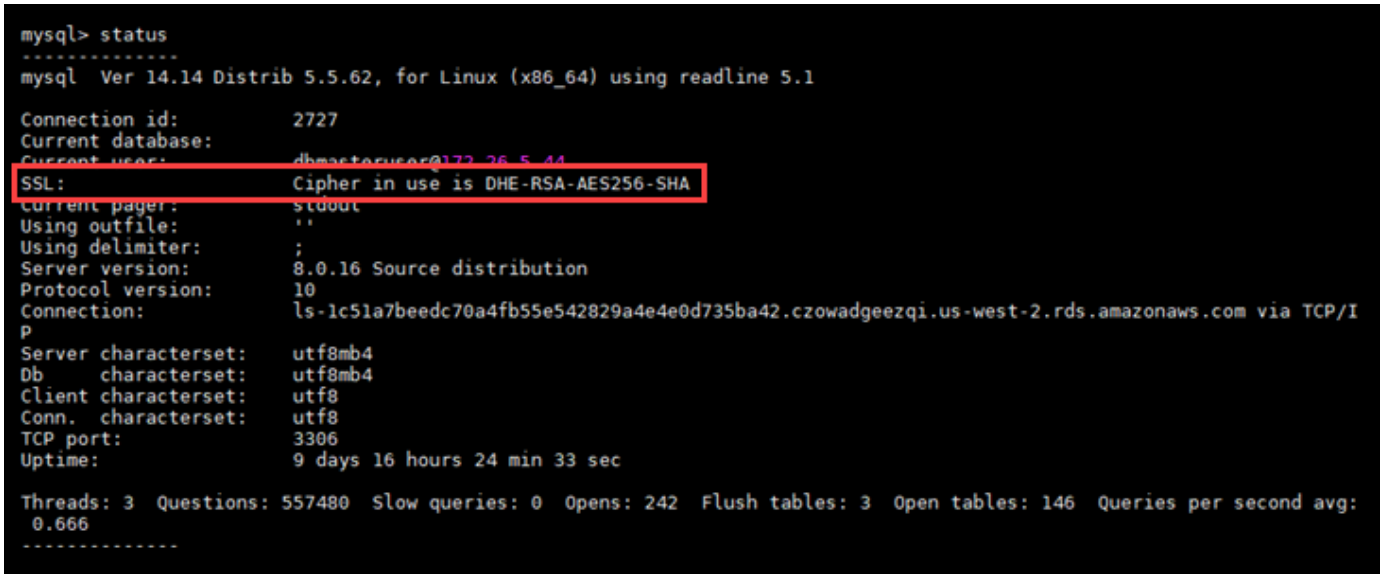
3. Geben Sie bei Aufforderung das Passwort für den Datenbankbenutzer ein, den Sie im vorherigen Befehl angegeben haben, und drücken Sie die Eingabetaste.

   Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:



4. Geben Sie **`status`** ein, und betätigen Sie die Eingabetaste, um den Status Ihrer Verbindung anzuzeigen.

   Ihre Verbindung ist verschlüsselt, wenn neben SSL der Wert „Cipher in use is“ angezeigt wird.



Herstellen einer Verbindung zu Ihrer Lightsail-PostgreSQL-Datenbank

Nachdem Ihre verwaltete PostGre-Datenbank in Amazon Lightsail erstellt wurde, können Sie jede standardmäßige PostGre-Clientanwendung oder ein Dienstprogramm verwenden, um sich mit ihr zu verbinden. Sie müssen den Datenbank-Endpunkt, den Port, den Benutzernamen und das Passwort von Ihrer Seite zur Datenbankverwaltung in der Lightsail-Konsole abrufen. Geben Sie diese Werte bei der Konfiguration der Datenbankverbindung in Ihrem Client oder Ihrer Webanwendung an.

Diese Anleitung zeigt Ihnen, wie Sie die erforderlichen Verbindungsinformationen erhalten und wie Sie den pgAdmin-Client so konfigurieren, dass er sich mit Ihrer verwalteten Datenbank verbindet.

> **Note**
>
> Weitere Informationen zum Herstellen einer Verbindung zu einer MySQL-Datenbank finden Sie unter Herstellen einer Verbindung mit Ihrer MySQL-Datenbank.

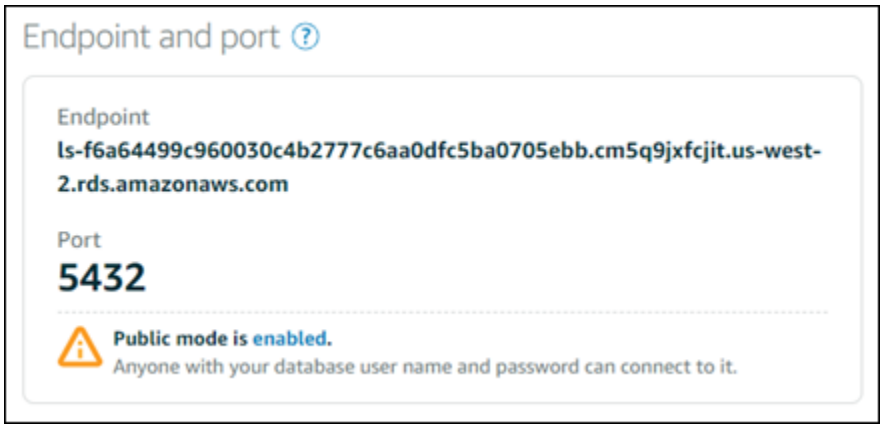
Schritt 1: Abrufen der Daten für Ihre PostGreSQL-Datenbankverbindung

Holen Sie sich Ihre Datenbank-Endpunkt- und Port-Informationen aus der Lightsail-Konsole. Diese verwenden Sie später bei der Konfiguration Ihres Clients für die Verbindung mit Ihrer Datenbank.

So erhalten Sie Ihre Datenbankverbindungsdaten

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Databases (Datenbanken) aus.
3. Wählen Sie den Namen der Datenbank aus, mit der Sie sich verbinden möchten.
4. Notieren Sie sich auf der Registerkarte Connect (Verbinden) unter dem Abschnitt Endpoint and port (Endpunkt und Port) die Informationen zu Endpunkt und Port.

   Wir empfehlen, den Endpunkt in die Zwischenablage zu kopieren, um eine falsche Eingabe zu vermeiden. Markieren Sie dazu den Endpunkt und drücken Sie Ctrl+C (Strg+C), wenn Sie Windows verwenden, oder Cmd+C, wenn Sie MacOS verwenden, um ihn in die Zwischenablage zu kopieren. Drücken Sie dann Strg+V oder Cmd+V, um ihn einzufügen.

5. Klicken Sie auf der Registerkarte Connect (Verbinden) im Abschnitt User name and passwords (Benutzername und Passwörter), notieren Sie sich den Benutzernamen, und wählen Sie dann Show (Anzeigen) unter dem Abschnitt Password (Passwort), um das aktuelle Datenbankpasswort anzuzeigen.

   Da verwaltete Passwörter komplex sind, empfehlen wir, sie zu kopieren und einzufügen, um eine falsche Eingabe zu vermeiden. Markieren Sie das verwaltete Passwort und drücken Sie Ctrl+C (Strg+C), wenn Sie Windows verwenden, oder Cmd+C, wenn Sie MacOS verwenden, um es in die Zwischenablage zu kopieren. Drücken Sie dann Strg+V oder Cmd+V, um ihn einzufügen.

Schritt 2: Konfigurieren der öffentliche Verfügbarkeit Ihrer PostGreSQL-Datenbank

Sie müssen den öffentlichen Modus aktivieren, damit sich Ihre Datenbank extern oder von einer Lightsail-Instance in einer anderen Region als Ihrer Datenbank mit ihr verbinden kann. Wenn der

öffentliche Modus aktiviert ist, kann sich jeder mit dem Datenbankbenutzernamen und dem Passwort mit Ihrer Datenbank verbinden. Um die öffentliche Verfügbarkeit Ihrer Datenbank zu konfigurieren, befolgen Sie die Schritte im Handbuch Konfigurieren des öffentlichen Modus für Ihre Datenbank.

> **Note**
>
> Gehen Sie zu Schritt 3 über, wenn Sie eine Verbindung zu Ihrer Datenbank von einer Ihrer Lightsail-Instances aus planen, die sich in derselben Region wie Ihre Datenbank befindet.

Schritt 3: Konfigurieren Ihres Datenbank-Clients für die Verbindung mit Ihrer PostGreSQL-Datenbank

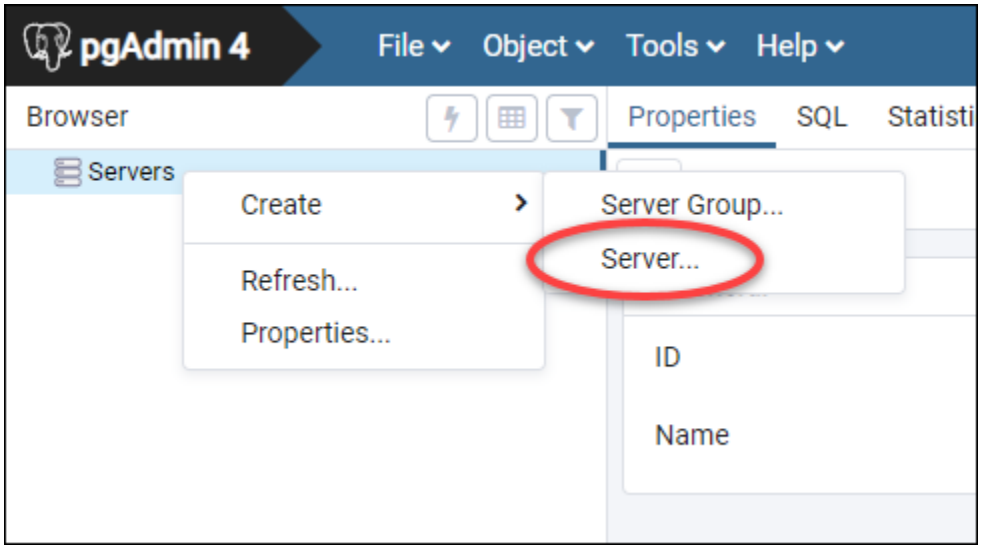
Um eine Verbindung zu Ihrer PostGreSQL-Datenbank herzustellen, konfigurieren Sie Ihren Datenbank-Client so, dass er den Endpunkt und den Port verwendet, den Sie zuvor erhalten haben. Die folgenden Schritte veranschaulichen, wie Sie pgAdmin konfigurieren, diese Schritte sind aber möglicherweise sehr ähnlich mit denen für andere Clients.

> **Note**
>
> Weitere Informationen zur Verwendung von pgAdmin finden Sie in der pgAdmin-Dokumentation.

So konfigurieren Sie pgAdmin, um eine Verbindung mit Ihrer Datenbank herzustellen:

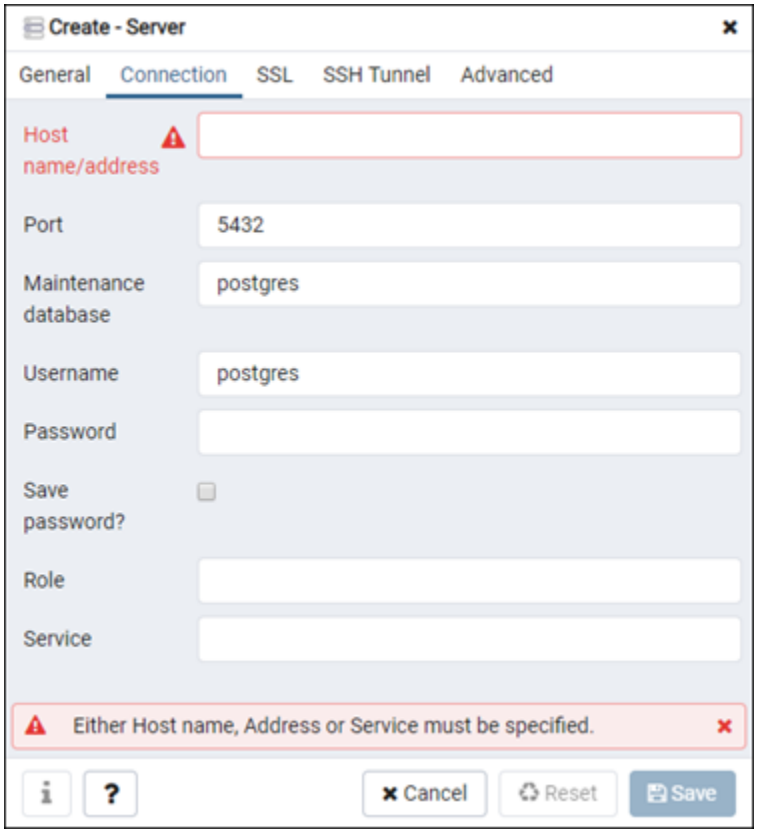
1. Öffnen Sie pgAdmin.
2. Klicken Sie mit der rechten Maustaste auf Servers (Server) im linken Navigationsmenü.
3. Wählen Sie Create (Erstellen), und klicken Sie dann auf Server.

4.



5. Geben Sie im Formular Create - Server (Erstellen - Server) einen Namen für den Server ein. Wir empfehlen, einen Namen für die Verbindung zu verwenden, der dem Ihrer Datenbank ähnlich ist. Dies hilft Ihnen, sie in Zukunft zu identifizieren.

6. Wählen Sie die Registerkarte Connection (Verbindung) und geben Sie in dem angezeigten Formular die folgenden Informationen ein:



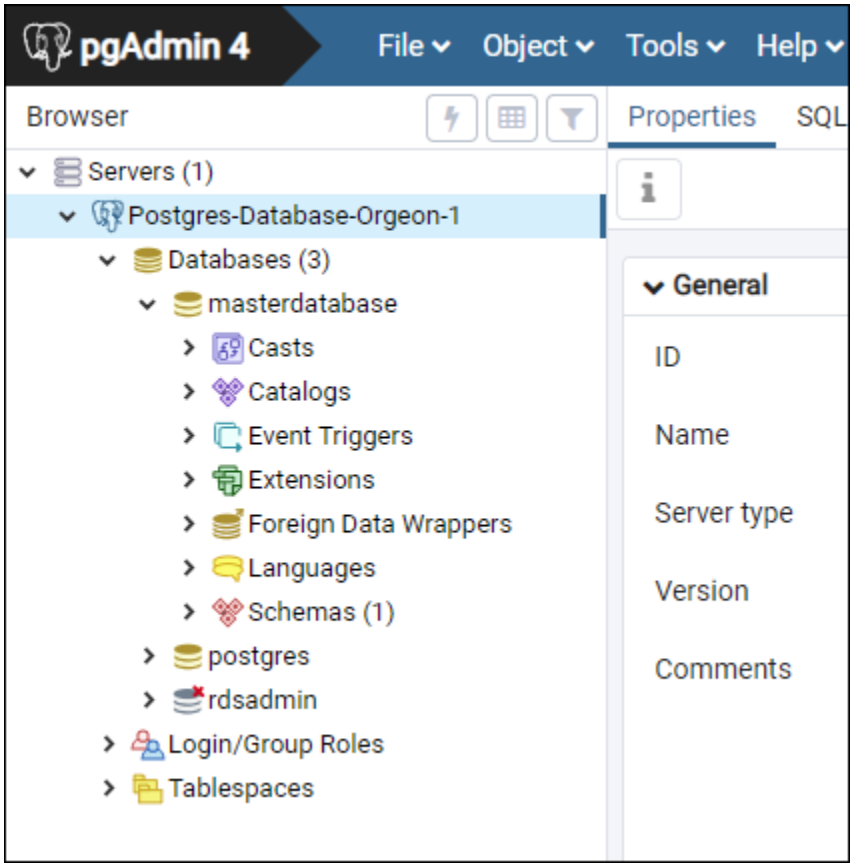
- Host name/address (Hostname/-adresse) - Geben Sie den Datenbankendpunkt ein, den Sie vorher erhalten haben. Wenn Sie den Datenbank-Endpunkt aus der Lightsail-Konsole kopiert haben und er sich noch in der Zwischenablage befindet, drücken Sie Strg+V, wenn Sie Windows verwenden, oder Cmd+V, wenn Sie MacOS verwenden, um ihn einzufügen.
- Port – Geben Sie den Port für Ihre Datenbank ein, den Sie zuvor erhalten haben. Der Standardwert für PostgreSQL lautet 5432.
- Maintenance Datenbank (Wartungsdatenbank) – Geben Sie den Namen der anfänglichen Datenbank ein, zu dem der Client eine Verbindung herstellt. Dies ist der primäre Datenbankname, den Sie beim Erstellen Ihrer PostgreSQL-Datenbank in Lightsail angegeben haben.

  Geben Sie `postgres` ein, wenn Sie sich nicht an den Namen der primären Datenbank erinnern. Jede PostgreSQL-verwaltete Datenbank ist eine `postgres`-Datenbank, mit der Sie eine Verbindung herstellen können; anschließend können Sie auf alle anderen Datenbanken auf der PostgreSQL-verwalteten Datenbank zugreifen.
- Username (Benutzername) – Geben Sie den Datenbankbenutzernamen ein, den Sie zuvor erhalten haben.
- Password (Passwort) – Geben Sie Ihr Datenbankpasswort ein, das Sie zuvor erhalten haben. Wenn Sie das Passwort aus der Lightsail-Konsole kopiert haben und es sich noch in der Zwischenablage befindet, drücken Sie Strg+V, wenn Sie Windows verwenden, oder Cmd +V, wenn Sie MacOS verwenden, um es einzufügen. Wählen Sie Save password (Passwort speichern), um das Passwort zu speichern.
- Role (Rolle) und Service – Lassen Sie diese Felder leer.

7. Wählen Sie Save (Speichern) um die neuen Server-Details zu speichern.

   Ihre neue Datenbankverbindung wird im linken Navigationsmenü der Anwendung pgAdmin unter dem Abschnitt „Server“ aufgeführt.
8. Doppelklicken Sie auf Ihre neue Datenbankverbindung, um eine Verbindung zu Ihrer Datenbank herzustellen.

   Wenn die Verbindung erfolgreich ist, sehen Sie eine Liste der verfügbaren Ressourcen für diese Datenbank.



Nächste Schritte

Hier ist eine Anleitung, die Ihnen hilft, Daten in Ihre Datenbank in Lightsail zu importieren:

- Importieren von Daten in Ihre PostgreSQL-Datenbank

Mit SSL eine Verbindung zu Ihrer Lightsail-PostgreSQL-Datenbank herstellen

Amazon Lightsail erstellt ein SSL-Zertifikat und installiert es in der von PostgreSQL (Postgres) verwalteten Datenbank, wenn es bereitgestellt wird. Das Zertifikat ist von einer Zertifizierungsstelle (Certificate Authority, CA) signiert und enthält den Datenbankendpunkt als Common Name (CN) für das SSL-Zertifikat, um vor Spoofing-Angriffen zu schützen.

Ein SSL-Zertifikat, das von Lightsail erstellt wurde, ist die vertrauenswürdige Root Entity und sollte in den meisten Fällen funktionieren, könnte jedoch fehlschlagen, wenn Ihre Anwendung keine

Zertifikatsketten akzeptiert. Wenn Ihre Anwendung keine Zertifikatsketten akzeptiert, müssen Sie evtl. ein Zwischenzertifikat verwenden, um sich mit Ihrer AWS-Region zu verbinden.

Weitere Informationen zu den CA-Zertifikaten für die verwaltete Datenbank, zu den unterstützten AWS-Regionen und zum Herunterladen von Zwischenzertifikaten für Ihre Anwendungen finden Sie unter Herunterladen eines SSL-Zertifikats für Ihre verwaltete Datenbank.

Voraussetzungen

- Installieren Sie PostgreSQL Server auf dem Computer, mit dem Sie eine Verbindung zu Ihrer Datenbank herstellen. Weitere Informationen finden Sie unter PostgreSQL-Downloads auf der Postgres-Website
- Laden Sie das entsprechende Zertifikat für Ihre Datenbank herunter. Weitere Informationen finden Sie unter Herunterladen eines SSL-Zertifikats für die verwaltete Datenbank.

Verbinden Sie sich mit Ihrer Postgres-Datenbank mit SSL

Führen Sie die folgenden Schritte aus, um eine Verbindung mit Ihrer Postgres-Datenbank mithilfe von SSL herzustellen.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um eine Verbindung mit einer PostgreSQL-Datenbank herzustellen.

   ```
   psql -h DatabaseEndpoint -p 5432 "dbname=DatabaseName user=UserName sslrootcert=/
   path/to/certificate/rds-combined-ca-bundle.pem sslmode=verify-full"
   ```

   Ersetzen Sie im Befehl Folgendes:

   - *DatabaseEndpoint* mit dem Endpunkt Ihrer Datenbank.
   - *DatabaseName* durch den Namen der Datenbank, mit der Sie eine Verbindung herstellen möchten.
   - *UserName* mit dem Benutzernamen Ihrer Datenbank.
   - */path/to/certificate/rds-combined-ca-bundle.pem* mit dem lokalen Pfad, in dem Sie das Zertifikat für Ihre Datenbank heruntergeladen und gespeichert haben.

   Beispiel:

```
psql -h ls-8e81e07f8b821917b11e1c6a0e26cb73c203.czowadgeezqi.us-
west-2.rds.amazonaws.com -p 5432 "dbname=dbmaster user=dbmasteruser sslrootcert=/
home/ec2-user/rds-combined-ca-bundle.pem sslmode=verify-full"
```

3. Geben Sie bei Aufforderung das Passwort für den Datenbankbenutzer ein, den Sie im vorherigen Befehl angegeben haben, und drücken Sie die Eingabetaste.

   Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten: Ihre Verbindung wird verschlüsselt, wenn der Wert „SSL-Verbindung“ angezeigt wird.

Löschen Ihrer Lightsail-Datenbank

Löschen Sie Ihre verwaltete Datenbank in Amazon Lightsail, wenn Sie sie nicht mehr benötigen. Sobald die Datenbank gelöscht wurde, fallen keine weiteren Kosten für sie mehr an.

> **Note**
>
> Sie können eine gelöschte Datenbank nicht wiederherstellen. Sie können einen finalen Snapshot Ihrer Datenbank im Rahmen der in diesem Handbuch beschriebenen Schritte erstellen oder einen Snapshot separat vom Löschvorgang erstellen. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Datenbank

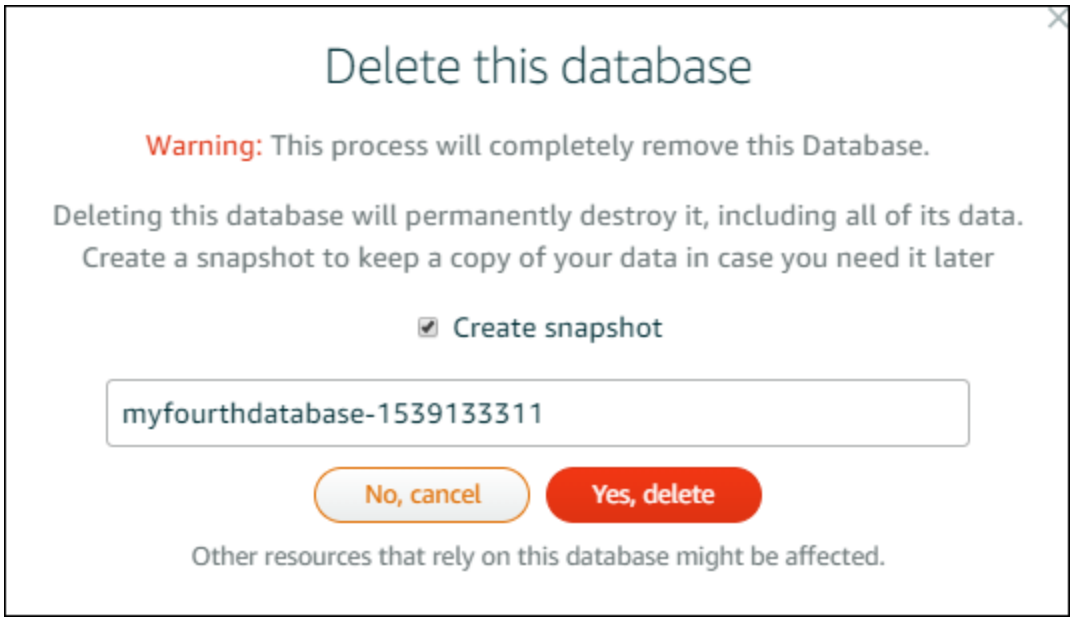
So löschen Sie Ihre Datenbank

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Databases (Datenbanken) aus.
3. Wählen Sie den Namen der Datenbank, die Sie löschen möchten.
4. Wählen Sie die Registerkarte Delete (Löschen) aus.

5. Fügen Sie ein Häkchen neben Snapshot vor dem Löschen erstellen hinzu, um einen finalen Snapshot vor dem Löschen der Datenbank zu erstellen. Geben Sie dann einen Namen für Ihren Snapshot ein.

   Ressourcennamen:

   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.
6. Wählen Sie Delete database (Datenbank löschen) aus.
7. Wählen Sie Yes, delete (Ja, löschen) zum Bestätigen der Löschung aus.



   Wenn Sie sich vor dem Löschen für die Erstellung eines Snapshots entschieden haben, können Sie diesen auf der Registerkarte Snapshots der Lightsail-Startseite ansehen.

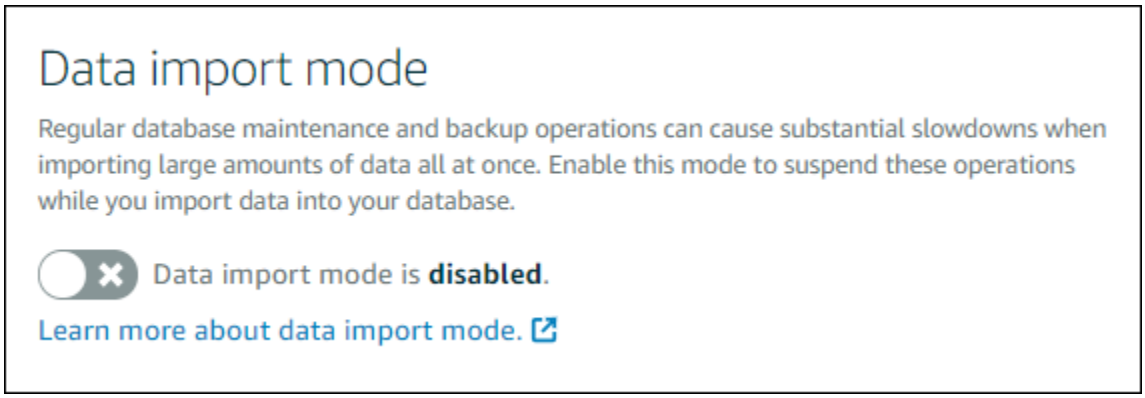
Konfigurieren des Datenimportmodus für Ihre Lightsail-Datenbank

Regelmäßige Datenbanksicherungsvorgänge können beim Import großer Datenmengen zu erheblichen Verzögerungen oder Leistungsabfällen führen. Aktivieren Sie den Datenimportmodus für Ihre verwaltete Amazon Lightsail-Datenbank, um diese Vorgänge auszusetzen, während Sie große Datenmengen importieren.

> **Important**
>
> Alle Notfall-Wiederherstellungen von Sicherungen werden gelöscht, wenn der Datenimportmodus aktiviert ist. Erstellen Sie einen Snapshot Ihrer Datenbank, wenn Sie eine Sicherung wünschen, bevor der Datenimportmodus aktiviert wird. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Datenbank

So konfigurieren Sie den Datenimportmodus für Ihre Datenbank:

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Databases (Datenbanken) aus.
3. Wählen Sie den Namen der Datenbank aus, für die Sie den Datenimportmodus konfigurieren möchten.
4. Verwenden Sie auf der Registerkarte Connect (Verbinden) unter dem Abschnitt Data import mode (Datenimportmodus) den Schalter, um den Datenimportmodus einzuschalten. Nachdem der Import abgeschlossen ist, schalten Sie ihn mit dem Schalter aus.



   Wenn der Datenimportmodus aktiviert ist, werden die Datenbanksicherungsvorgänge ausgesetzt. Wir empfehlen Ihnen, den Datenimportmodus vorübergehend zu aktivieren. Verwenden Sie ihn nur dann, wenn es erforderlich ist, dass Sie große Datenmengen in Ihre Datenbank importieren. Deaktivieren Sie den Datenimportmodus, sobald Sie fertig sind, um die Sicherungsvorgänge wieder zu aktivieren.

   > **Note**
   >
   > Ihr Import kann sich abhängig von der Menge der Daten, die Sie importieren, verlangsamen. Weitere Informationen finden Sie unter Optimieren des Datenimports.

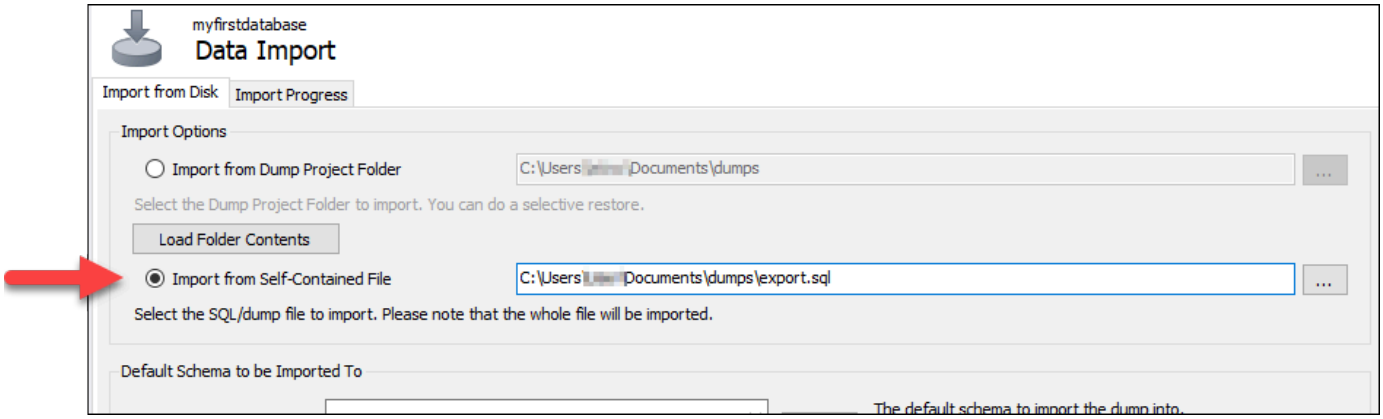
Importieren von Daten in Ihre MySQL-Datenbank in Lightsail

Sie können mit MySQL Workbench eine SQL-Datei (.SQL) in Ihre MySQL verwaltete Datenbank in Amazon Lightsail importieren.

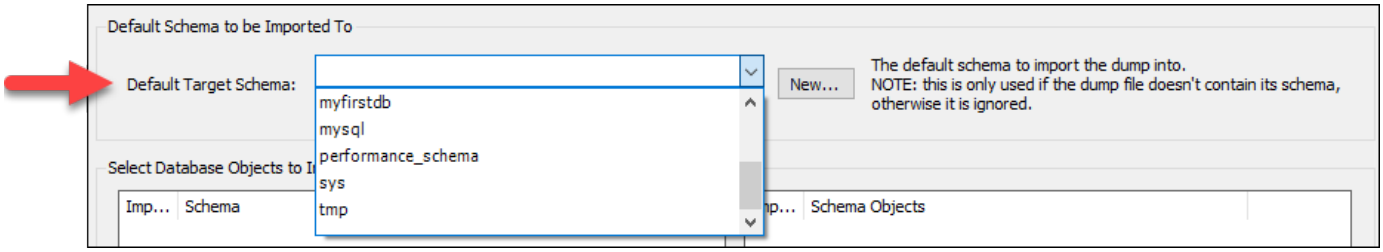
> **Note**
>
> Weitere Informationen wie Sie MySQL Workbench mit Ihrer Datenbank verbinden, finden Sie unter Herstellen einer Verbindung zu Ihrer MySQL-Datenbank.

So importieren Sie Daten in Ihre Datenbank

1. Öffnen Sie MySQL Workbench.
2. Wählen Sie in der Liste der MySQL-Verbindungen Ihre MySQL-verwaltete Datenbank aus.
3. Wählen Sie Data Import/Restore (Datenimport/Wiederherstellen) aus dem linken Navigationsmenü.
4. Wählen Sie im Bereich Datenimport Import from Self-Contained File (Importieren aus einer eigenständigen Datei) unter dem Abschnitt Import Options (Importoptionen) aus.

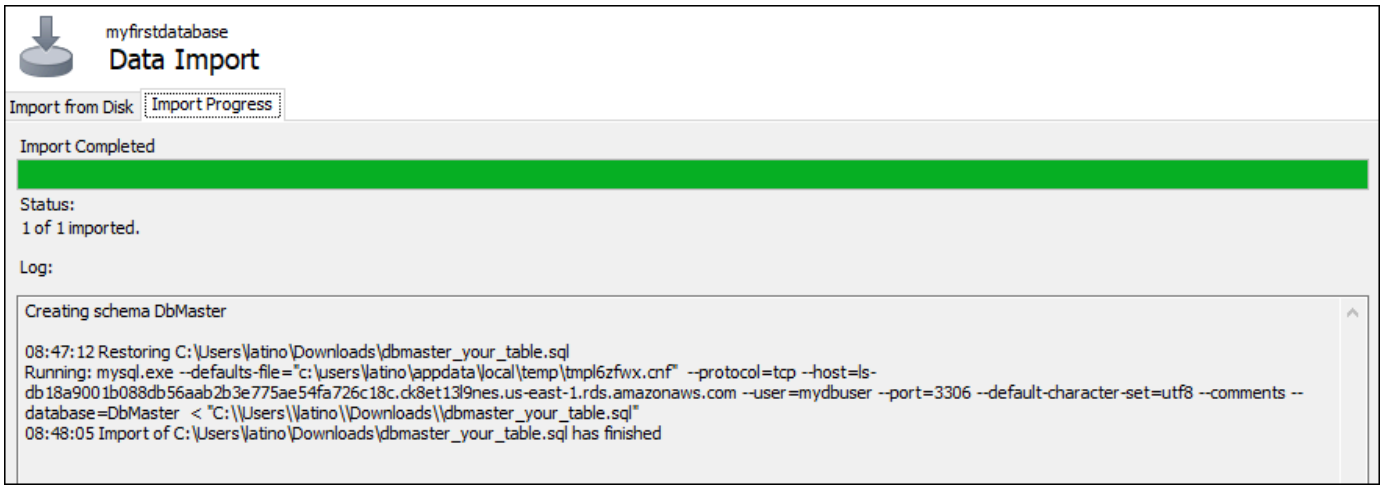


5. Klicken Sie auf die Ellipsenschaltfläche, um Ihr lokales Laufwerk nach der SQL-Datei zu durchsuchen, die Sie importieren möchten.
6. Wählen Sie die zu importierende SQL-Datei aus und dann Open (Öffnen).
7. Wählen Sie im Dropdown-Menü Default Target Schema (Standard-Zielschema) aus und wählen Sie dann die bestehende Datenbank, um die Datei zu importieren. Sie können auch eine neue Datenbank erstellen, indem Sie New (Neu) auswählen.



8. Wählen Sie Start Import (Import starten), um den Import zu starten.

   Der Import kann je nach Größe der SQL-Datei einige Minuten oder auch länger dauern. Nach Abschluss des Imports sollten Sie eine Meldung ähnlich der folgenden erhalten:



Importieren von Daten in Ihre PostgreSQL-Datenbank in Lightsail

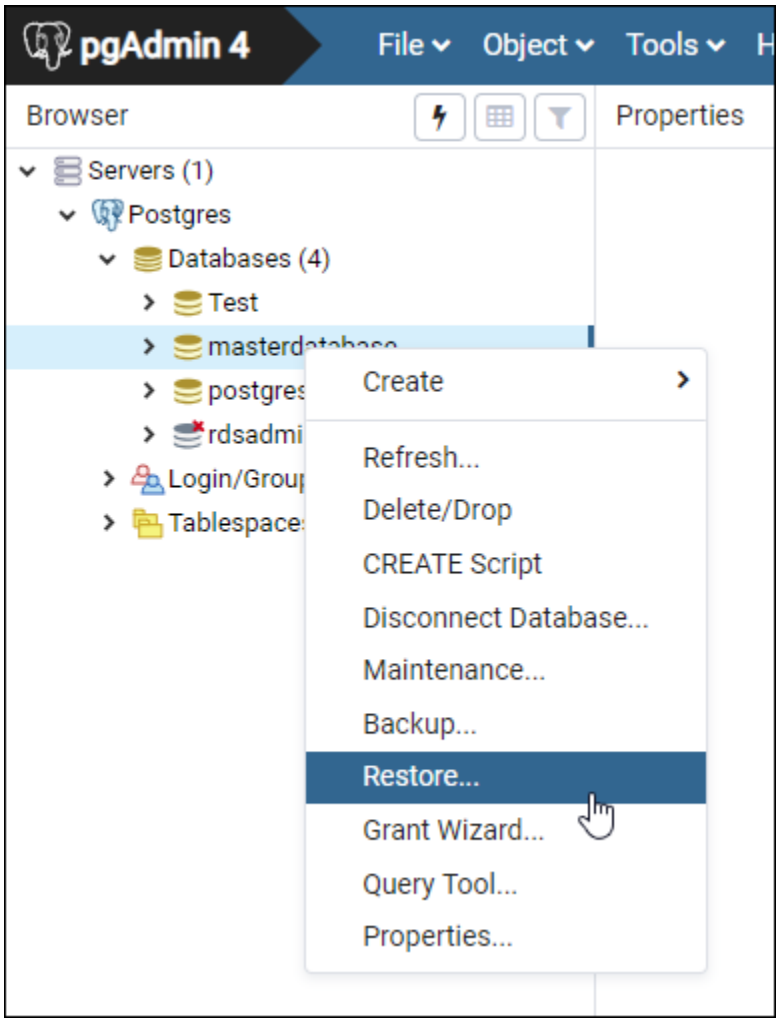
Sie können eine Datenbank-Backup-Datei mit pgAdmin in Ihre von PostgreSQL verwaltete Datenbank in Amazon Lightsail importieren.

> **Note**
>
> Weitere Informationen wie Sie pgAdmin mit Ihrer Datenbank verbinden, finden Sie unter Herstellen einer Verbindung zu einer PostgreSQL-Datenbank. Weitere Informationen zum Erstellen eines PostgreSQL-Datenbank-Backups, das Sie in eine andere Datenbank importieren können, finden Sie unter Backup-Dialog in der pgAdmin-Dokumentation.

So importieren Sie eine Backup-Datei in Ihrer Datenbank

1. Öffnen Sie pgAdmin.

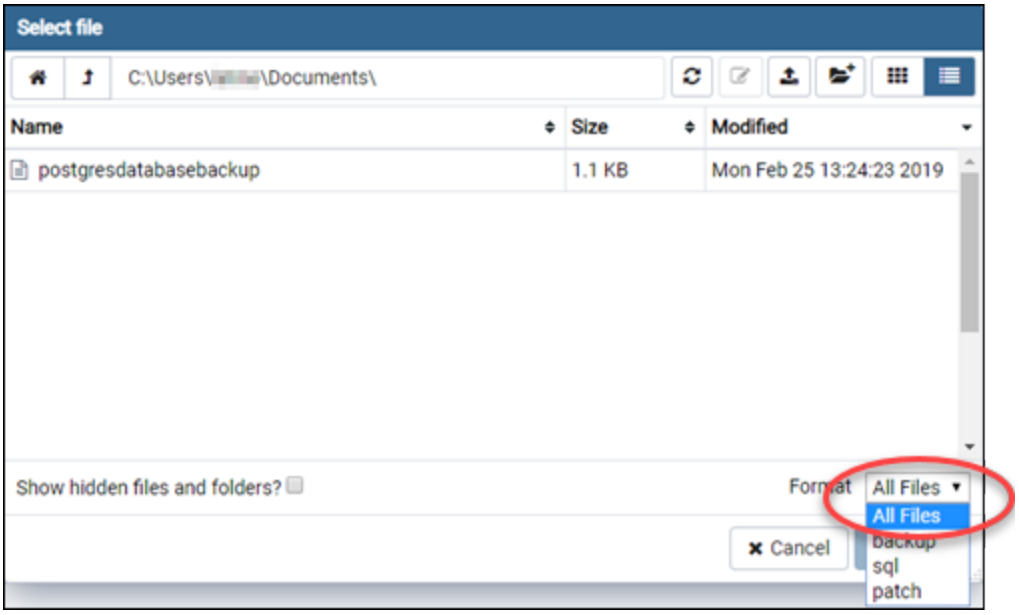
2. Doppelklicken Sie in der Liste der Serververbindungen auf Ihre von PostgreSQL verwaltete Datenbank in Amazon Lightsail, um eine Verbindung herzustellen.
3. Erweitern Sie den Knoten der Databases (Datenbanken)
4. Klicken Sie mit der rechten Maustaste auf die Datenbank, in die Sie die Daten aus einer Datenbank-Backup-Datei importieren möchten, und wählen Sie dann Restore (Wiederherstellen).



5. Füllen Sie im Formular Restore (Wiederherstellen) die folgenden Felder aus:

   - Format – Wählen Sie das Format Ihrer Backup-Datei.
   - Filename (Dateiname) – Klicken Sie auf das Symbol mit den drei Auslassungspunkten, und suchen und wählen Sie die Datenbank-Backup-Datei auf Ihrem lokalen Laufwerk. Nachdem die Datei markiert ist, wählen Sie Select (Auswählen), um zur Restore (Wiederherstellen) Eingabeaufforderung zurückzukehren.

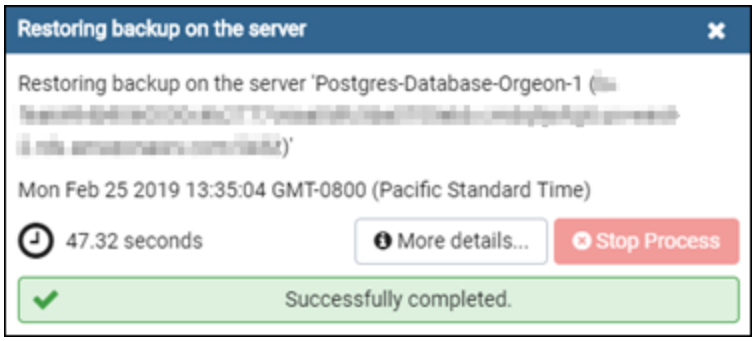
> **Note**
>
> Klicken Sie auf das Dropdown-Menü Format und wählen Sie All files (Alle Dateien), um alle Dateiformate auf Ihrem lokalen Laufwerk anzuzeigen. Ihre Backup-Datei kann in einem Dateityp vorliegen, der nicht standardmäßig ausgewählt ist (sql).



- Number of jobs (Anzahl der Aufgaben) und Role name (Rollenname) – Lassen Sie diese Felder leer.

6. Wählen Sie Restore (Wiederherstelen) um den Import zu starten.

   Der Import kann einige Minuten oder länger dauern, abhängig von der Größe der Datenbank-Backup-Datei. Nach Abschluss des Imports sollten Sie eine Meldung ähnlich der folgenden erhalten:



Anzeigen Ihrer Lightsail-Datenbankprotokolle und Ihres Verlaufs

Zeigen Sie Ihre Datenbankprotokolle und den Änderungsverlauf in der Amazon Lightsail-Konsole an. Database Protokolle könnten nützliche Informationen, die Ihnen dabei helfen, Probleme mit Ihrer Datenbank zu diagnostizieren. Die Datenbankhistorie zeigt auch Ihre Änderungen an Ihrer Datenbank an, so dass Sie Probleme mit einer aktuellen Änderung in Verbindung bringen können.

So zeigen Sie Ihre Datenbankprotokolle an

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Databases (Datenbanken) aus.
3. Wählen Sie den Namen der Datenbank, für die Sie die Protokolle anzeigen möchten.
4. Wählen Sie die Registerkarte Logs and history (Protokolle und Historie).

   Die Seite zeigt die Datenbankprotokolle und die Historie der vorgenommenen Änderungen an Ihrer Datenbank an.
5. Wählen Sie ein Datenbankprotokoll aus. Die folgenden Datenbankprotokolle sind verfügbar:

   MySQL Datenbankprotokolle

   - Fehlerprotokoll – Das Fehlerprotokoll enthält einen Datensatz der Zeiten beim Starten und Herunterfahren von mysqld. Es enthält auch diagnostische Meldungen, wie z. B. Fehler, Warnungen und Hinweise, die beim Starten und Herunterfahren während der Ausführung des Servers auftreten. Weitere Informationen finden Sie im Artikel zum Fehlerprotokoll in der MySQL 5.6, MySQL 5.7- oder MySQL 8.0-Dokumentation.
   - General log — Das allgemeine Protokoll ist ein allgemeiner Datensatz der von mysqld ausgeführten Aufgaben. Der Server schreibt Informationen in dieses Protokoll, wenn Clients verbunden oder getrennt werden, und es protokolliert alle von Clients empfangenen SQL-Anweisungen. Weitere Informationen finden Sie im Artikel zum Allgemeinen Abfrageprotokoll in der MySQL 5.6, MySQL 5.7- oder MySQL 8.0-Dokumentation.
   - Slow query log — Das Slow-Query-Protokoll besteht aus SQL-Anweisungen, für deren Ausführung mehr als long_query_time Sekunden benötigt wurden und mindestens min_examined_row_limit Zeilen überprüft werden mussten. Weitere Informationen finden Sie im Artikel zum Slow-Query-Protokoll in der MySQL 5.6, MySQL 5.7- oder MySQL 8.0-Dokumentation.

> **Note**
>
> Das allgemeine Protokoll und das Slow-Query-Protokoll sind für MySQL-Datenbanken standardmäßig deaktiviert. Sie können diese Protokolle aktivieren und mit dem Sammeln von Daten beginnen, indem Sie ein paar Datenbankparameter aktualisieren. Weitere Informationen finden Sie unter Aktivieren der allgemeinen und langsamen Abfrageprotokolle in Amazon Lightsail.

PostgreSQL-Datenbankprotokolle

- Postgres-Protokoll – Eine Aufzeichnung der Start- und Abschaltzeiten der Datenbank. Es können auch Diagnosen wie Fehler, Warnungen, Benachrichtigungen und Debug-Meldungen enthalten sein, die beim Starten, Herunterfahren und während des Datenbankbetriebs auftreten. Weitere Informationen finden Sie im Artikel zu Fehlerberichterstattung und Protokollierung in der Dokumentation zu PostgreSQL 9.6, PostgreSQL 10, PostgreSQL 11 oder PostgreSQL 12.

Themen

Aktivieren allgemeiner und langsamer Abfrageprotokolle für Ihre Lightsail-MySQL-Datenbank

Die allgemeinen und Slow-Query-Protokolle sind für MySQL-Datenbanken in Amazon Lightsail standardmäßig deaktiviert. Sie können diese Protokolle aktivieren und mit dem Sammeln von Daten beginnen, indem Sie ein paar Datenbankparameter aktualisieren. Aktualisieren Sie die Datenbankparameter mithilfe der Lightsail-API, AWS Command Line Interface (AWS CLI) oder SDKs. In diesem Handbuch zeigen wir Ihnen, wie Sie mit der AWS CLI Ihre Datenbankparameter aktualisieren und die allgemeinen und Slow-Query-Protokolle aktivieren. Wir bieten außerdem zusätzliche Optionen für die Kontrolle der allgemeinen und Slow-Query-Protokolle und für die Handhabung der Protokolldatenaufbewahrung.

Voraussetzung

Falls noch nicht erfolgt, installieren und konfigurieren Sie die AWS CLI. Weitere Informationen finden Sie unter Konfigurieren der AWS Command Line Interface für die Arbeit mit Amazon Lightsail.

Aktivieren der allgemeinen und Slow-Query-Protokolle in der Lightsail-Konsole

Um die allgemeinen und Slow-Query-Protokolle in der Lightsail-Konsole zu aktivieren, müssen Sie die `slow_query_log` Datenbankparameter `general_log` und mit dem Wert `1`und den `log_output` Parameter mit dem Wert aktualisieren`FILE`.

So aktivieren Sie die allgemeinen und Slow-Query-Protokolle in der Lightsail-Konsole

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl zum Aktualisieren des Parameters `general_log` auf den Wert 1, der "wahr" oder "aktiviert" bedeutet, ein.

   ```
   aws lightsail update-relational-database-parameters --
   region Region --relational-database-name DatabaseName --parameters
    "parameterName=general_log,parameterValue=1,applyMethod=pending-reboot"
   ```

   Ersetzen Sie im Befehl Folgendes:

   - *DatabaseName* durch den Namen Ihrer Datenbank.
   - *Region* mit der AWS-Region Ihrer Datenbank.
3. Geben Sie den folgenden Befehl zum Aktualisieren des Parameters `slow_query_log` auf den Wert 1, der "wahr" oder "aktiviert" bedeutet, ein.

   ```
   aws lightsail update-relational-database-parameters --
   region Region --relational-database-name DatabaseName --parameters
    "parameterName=slow_query_log,parameterValue=1,applyMethod=pending-reboot"
   ```

   Ersetzen Sie im Befehl Folgendes:

   - *DatabaseName* durch den Namen Ihrer Datenbank.
   - *Region* mit der AWS-Region Ihrer Datenbank.

4. Geben Sie den folgenden Befehl ein, um den `log_output` Parameter auf einen Wert von zu aktualisieren`FILE`, der die Protokolldaten in eine Systemdatei schreibt und es ermöglicht, sie in der Lightsail-Konsole anzuzeigen.

```
aws lightsail update-relational-database-parameters --
region Region --relational-database-name DatabaseName --parameters
 "parameterName=log_output,parameterValue=FILE,applyMethod=pending-reboot"
```

   Ersetzen Sie im Befehl Folgendes:

   - *DatabaseName* durch den Namen Ihrer Datenbank.
   - *Region* mit der AWS-Region Ihrer Datenbank.

5. Geben Sie den folgenden Befehl ein, um die Datenbank neu starten, damit die Änderungen wirksam werden.

```
aws lightsail reboot-relational-database --region Region --relational-database-
name DatabaseName
```

   Ersetzen Sie im Befehl Folgendes:

   - *DatabaseName* durch den Namen Ihrer Datenbank.
   - *Region* mit der AWS-Region Ihrer Datenbank.

   An diesem Punkt ist die Datenbank nicht mehr verfügbar, während sie neu gestartet wird. Warten Sie einige Minuten und melden Sie sich dann bei der Lightsail-Konsole an, um die allgemeinen und langsamen Abfrageprotokolle für Ihre Datenbank anzuzeigen. Weitere Informationen finden Sie unter Anzeigen Ihrer Datenbankprotokolle und Ihres Verlaufs in Amazon Lightsail.

   > **Note**
   >
   > Weitere Informationen zum Aktualisieren von Datenbankparametern finden Sie unter Aktualisieren von Datenbankparametern in Amazon Lightsail.

Einstellen zusätzlicher Datenbankprotokolloptionen

Um zusätzliche Optionen für allgemeine und Slow-Query-Protokolle für MySQL einzustellen, aktualisieren Sie die folgenden Parameter:

- `log_output`: Stellen Sie diesen Parameter auf `TABLE` ein. Dadurch werden allgemeine Abfragen in die `mysql.general_log`-Tabelle und Slow-Queries in die `mysql.slow_log`-Tabelle geschrieben. Sie können den Parameter `log_output` auch auf `NONE` einstellen, um die Protokollierung zu deaktivieren.

  > **Note**
  >
  > Wenn Sie den `log_output` Parameter auf setzen, `TABLE` werden die allgemeinen und langsamen Abfrageprotokolldaten in der Lightsail-Konsole nicht angezeigt. Stattdessen müssen Sie die Tabellen `mysql.general_log` und `mysql.slow_log` in Ihrer Datenbank einsehen, die Protokolldaten anzuzeigen.

- `long_query_time`: Um zu vermeiden, dass schnell ausgeführte Abfragen im Slow-Query-Protokoll aufgenommen werden, legen Sie die kürzeste Ausführungszeit für eine einzutragende Abfrage in Sekunden fest. Der Standardwert liegt bei 10 Sekunden und der Minimumwert bei 0. Wenn der Parameter `log_output` auf `FILE` eingestellt ist, können Sie einen Gleitkommawert angeben, der die Mikrosekundenauflösung festlegt. Wenn der Parameter `log_output` auf `TABLE` eingestellt ist, können Sie einen Ganzzahlwert angeben, der die Sekundenauflösung festlegt. Nur Abfragen, deren Ausführungszeit den Wert des `long_query_time`-Parameters übersteigt, werden im Protokoll aufgenommen. Wenn Sie beispielsweise `long_query_time` auf 0,1 setzen, verhindert dies Einträge von allen Abfragen, die weniger als 100 Millisekunden lang ausgeführt werden.
- `log_queries_not_using_indexes`: Um alle Abfragen, die keinen Index für das Slow-Query-Protokoll verwenden, im Protokoll aufzunehmen, legen Sie als Wert 1 fest. Der Standardwert ist 0. Abfragen, die keinen Index verwenden, werden protokolliert, auch wenn ihre Ausführungszeit niedriger als der Wert des `long_query_time`-Parameters ist.

Protokolldatenaufbewahrung

Wenn die Protokollierung aktiviert ist, werden in regelmäßigen Zeitabständen Tabellenprotokolle rotiert oder Protokolldateien gelöscht. Dies ist eine Vorsichtsmaßnahme, um möglichst zu vermeiden, dass eine umfangreiche Protokolldatei die Datenbanknutzung blockiert oder die Leistung

beeinträchtigt. Wenn der `log_output`-Parameter auf `FILE` oder `TABLE` eingestellt ist, wird die Protokollierung wie folgt gehandhabt:

- Wenn die `FILE`-Protokollierung aktiviert ist, werden Protokolldateien stündlich geprüft und Protokolldateien, die älter als 24 Stunden sind, werden gelöscht. In einigen Fällen kann die Größe der verbleibenden kombinierten Protokolldatei nach dem Löschen die Schwelle von 2 % des zugeteilten Speicherplatzes für eine Datenbank überschreiten. In diesen Fällen werden die umfangreichsten Protokolldateien gelöscht, bis die Größe den Schwellenwert nicht mehr überschreitet.
- Wenn die `TABLE`-Protokollierung aktiviert ist, werden in einigen Fällen alle 24 Stunden Protokolltabellen überschrieben.

  Diese Rotation erfolgt, wenn der von den Tabellen-Protokollen verwendete Speicherplatz mehr als 20 Prozent des zugeteilten Speicherplatzes ausmacht oder wenn die Größe aller Protokolle zusammen mehr als 10 GB beträgt.

  Wenn der für eine Datenbank verwendete Speicherplatz 90 Prozent des Speicherplatzes überschreitet, der der Datenbank zugeteilt ist, werden die Schwellen für die Protokollrotation reduziert.

  Protokolltabellen werden rotiert, wenn der von den Tabellen-Protokollen verwendete Speicherplatz mehr als 10 % des zugewiesenen Speicherplatzes ausmacht oder wenn die Größe alle Protokolle zusammen mehr als 5 GB beträgt.

  Sie können das Ereignis `low_free_storage` abonnieren, um Benachrichtigungen zu erhalten, wenn Protokolltabellen rotiert werden, um Speicherplatz freizugeben.

  - Beim Rotieren von Protokolldateien wird die aktuelle Protokolltabelle in eine Sicherungsprotokolltabelle kopiert, und die Einträge in der aktuellen Protokolltabelle werden entfernt. Sofern bereits eine Sicherungsprotokolltabelle vorhanden ist, wird diese gelöscht, bevor die aktuelle Protokolltabelle ins Backup kopiert wird. Sie können die Sicherungsprotokolltabelle abfragen. Die Backup-Protokolltabelle für die `mysql.general_log`-Tabelle ist als `mysql.general_log_backup` benannt. Die Backup-Protokolltabelle für die `mysql.slow_log`-Tabelle ist als `mysql.slow_log_backup` benannt.
  - Sie können die `mysql.general_log`-Tabelle rotieren, indem Sie die Prozedur `mysql.rds_rotate_general_logprocedure` aufrufen. Sie können die `mysql.slow_log`-Tabelle rotieren, indem Sie die Prozedur `mysql.rds_rotate_slow_logprocedure` aufrufen.
  - Tabellenprotokolle werden während des Upgrades einer Datenbankversion rotiert.

Einen Snapshot Ihrer Lightsail-Datenbank erstellen

Sie können einen Snapshot Ihrer verwalteten Datenbank in Amazon Lightsail erstellen. Ein Snapshot ist eine Kopie Ihrer Datenbank, die Sie verwenden können, um sie bei Problemen wiederherzustellen. Sie können einen Snapshot außerdem verwenden, um eine neue Datenbank mit einem anderen Plan zu erstellen – z. B. einem Hochverfügbarkeits- oder Standardplan.

Wenn Sie einen Snapshot einer Standarddatenbank erstellen, ist die Datenbank (je nach Größe) einige Sekunden bis einige Minuten nicht verfügbar. Hochverfügbare Datenbanken sind von Snapshot-Operationen nicht betroffen, da der Snapshot mit der Standby-Datenbank erstellt wird.

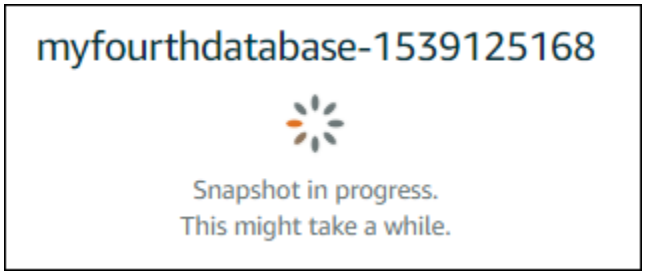
So erstellen Sie einen Snapshot Ihrer Datenbank

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Databases (Datenbanken) aus.
3. Wählen Sie den Namen der Datenbank, für die Sie einen Snapshot erstellen möchten.
4. Wählen Sie die Registerkarte Snapshots & restore (Snapshots und Wiederherstellung) aus.
5. Wählen Sie im Abschnitt Manual snapshots (Manuelle Snapshots) der Seite Create snapshot (Snapshot erstellen) und geben Sie dann einen Namen für Ihren Snapshot ein.

   Ressourcennamen:

   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.
6. Wählen Sie Erstellen aus.

   Der Prozess der Snapshot-Erstellung beginnt und es wird der Status von Snapshot in progress (Snapshot In Bearbeitung) angezeigt.



Nachdem der Prozess der Snapshot-Erstellung abgeschlossen ist, wird der neue Snapshot unter dem Abschnitt Recent snapshots (Kürzliche Snapshots) aufgelistet. Sie können außerdem alle Snapshots für Ihr Konto auf der Lightsail-Startseite unter der Registerkarte Snapshot anzeigen.

Nächste Schritte

Nachdem Ihr Snapshot fertig ist, können Sie aus dem Snapshot, der ein Duplikat der Originaldatenbank ist, eine neue Datenbank erstellen. Weitere Informationen finden Sie unter Erstellen einer Datenbank aus einem Snapshot.

Themen

- Eine Datenbank aus einer zeitpunktbezogenen Sicherung in Amazon Lightsail erstellen
- Eine Datenbank aus einem Snapshot in Lightsail erstellen

Eine Datenbank aus einer zeitpunktbezogenen Sicherung in Amazon Lightsail erstellen

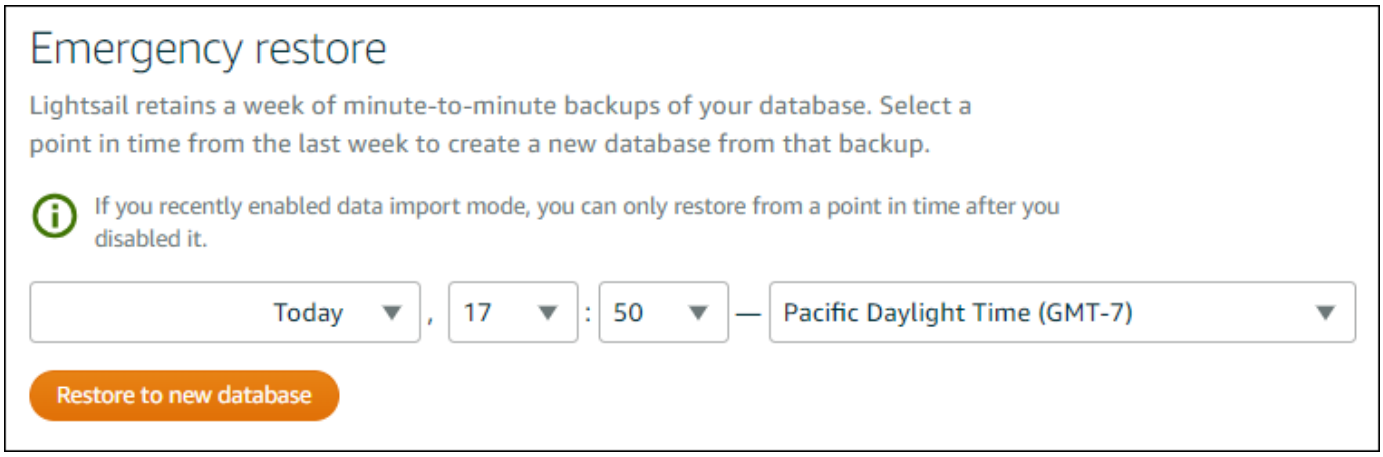
Sie können eine neue verwaltete Datenbank erstellen, indem Sie eine zeitpunktbezogene Sicherung in Amazon Lightsail verwenden. Zeitpunktbezogene Sicherungen Ihrer Datenbank sind in 5-Minuten-Schritten und für die letzten sieben Tage verfügbar. Dies gibt Ihnen die Möglichkeit, eine ausgefallene Datenbank auf ein bestimmtes Datum und eine bestimmte Uhrzeit in der letzten Woche wiederherzustellen.

Sie können außerdem eine neue Datenbank aus einem Snapshot erstellen. Weitere Informationen finden Sie unter Erstellen einer Datenbank aus einem Snapshot in Amazon Lightsail.

So erstellen Sie eine Datenbank aus einer zeitpunktbezogenen Sicherung

1. Melden Sie sich an der Lightsail-Konsole an.

2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Databases (Datenbanken) aus.
3. Wählen Sie den Namen der Datenbank aus, für die Sie die Pläne ändern möchten.
4. Wählen Sie die Registerkarte Snapshots and restore (Snapshots und Wiederherstellung).
5. Wählen Sie im Abschnitt Emergency restore (Notfallwiederherstellung) das Datum und die Uhrzeit der Sicherung aus, die Sie für Ihre neue Datenbank verwenden möchten.



6. Wählen Sie Restore to new database (Wiederherstellen in einer neuen Datenbank) aus.
7. Wählen Sie auf der Seite Create a new database (Eine neue Datenbank erstellen) die Option Change zone (Zone ändern) aus, um eine andere Availablity Zone auszuwählen. Ihre neue Datenbank wird dann in der AWS-Region erstellt, in der sich der zuvor ausgewählte Snapshot befindet.
8. Wählen Sie Ihren neuen Datenbankplan aus.

   Wählen Sie einen Hochverfügbarkeits- oder einen Standard-Datenbankplan aus. Eine mit einem Hochverfügbarkeitsplan erstellte Datenbank verfügt über eine primäre Datenbank und eine sekundäre Standby-Datenbank in einer anderen Availability Zone für die Failover-Unterstützung. Weitere Informationen finden Sie unter Hochverfügbarkeitsdatenbanken.

   > **Note**
   >
   > Sie können keinen Datenbankplan auswählen, der kleiner ist als der Plan der ursprünglichen Datenbank.

9. Geben Sie einen Namen für Ihre Datenbank ein.

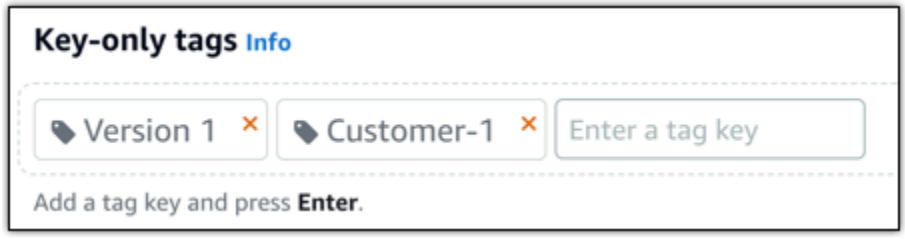
   Ressourcennamen:

   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.

- Muss zwischen 2 und 255 Zeichen enthalten.
- Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
- Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

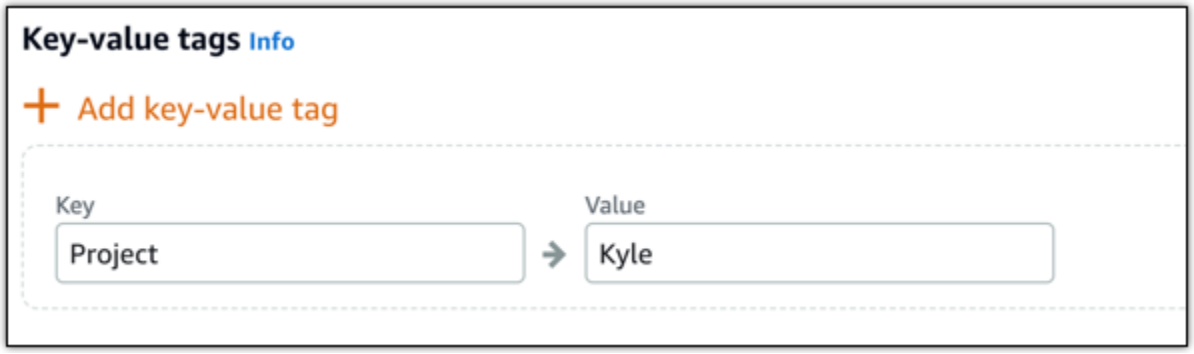
10. Wählen Sie eine der folgenden Optionen aus, um Ihrer Datenbank Tags hinzuzufügen:

    - Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.

    - Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

      Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.

> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

11. Wählen Sie Datenbank erstellen aus.

    Innerhalb weniger Minuten ist Ihre neue Lightsail-Datenbank mit dem neuen Datenbankplan oder -paket fertig.

Nächste Schritte

Führen Sie die folgenden Aktionen durch, nachdem Ihre neue Datenbank in Betrieb genommen wurde:

- Löschen Sie die Originaldatenbank, wenn Sie sie nicht mehr benötigen. Weitere Informationen finden Sie unter Löschen Ihrer Datenbank.
- Datenbanken, die aus einer zeitpunktbezogenen Sicherung erstellt wurden, sind so konfiguriert, dass sie ein von Lightsail erstelltes sicheres Passwort verwenden. Weitere Informationen finden Sie unter Verwaltung Ihres Datenbankpassworts.

Eine Datenbank aus einem Snapshot in Lightsail erstellen

Sie können eine neue verwaltete Datenbank aus einem Snapshot in Amazon Lightsail erstellen, wenn etwas mit Ihrer ursprünglichen Datenbank nicht stimmt. Sie können Ihre Datenbank auch auf einen anderen Plan ändern, z. B. auf einen Hochverfügbarkeits- oder Standardplan. Sie können außerdem eine neue Datenbank aus eine zeitbezogenen Sicherung Ihrer ursprünglichen Datenbank erstellen. Weitere Informationen finden Sie unter Erstellen einer Datenbank aus einer zeitpunktbezogenen Sicherung in Amazon Lightsail.

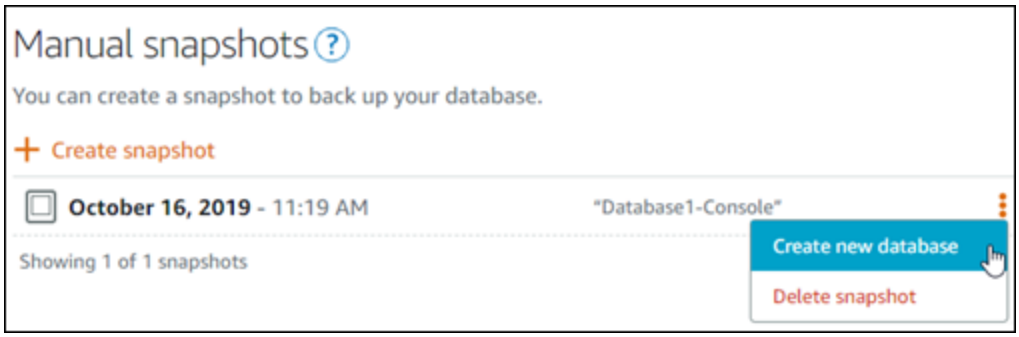
Wenn Sie eine duplizierte Datenbank erstellen, können Sie einen anderen oder größeren Plan als die ursprüngliche Datenbank auswählen. Sie können jedoch keinen kleineren Plan als den für die ursprüngliche Datenbank auswählen.

> **Note**
>
> Eine mit einem Hochverfügbarkeitsplan erstellte Datenbank verfügt über eine primäre Datenbank und eine sekundäre Standby-Datenbank in einer anderen Availability Zone für die Failover-Unterstützung. Weitere Informationen finden Sie unter Hochverfügbarkeitsdatenbanken.

So erstellen Sie eine Datenbank aus einem Snapshot

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Databases (Datenbanken) aus.
3. Wählen Sie den Namen der Datenbank aus, die Sie duplizieren möchten, indem Sie eine neue Datenbank aus einem Snapshot erstellen.
4. Wählen Sie die Registerkarte Snapshots & restore (Snapshots und Wiederherstellung) aus.
5. Wählen Sie im Abschnitt Manual snapshots (Manuelle Snapshots) der Seite das Aktionsmenüsymbol (⋮) neben dem Snapshot, aus dem Sie eine neue Datenbank erstellen möchten, und wählen Sie Create new database (Neue Datenbank erstellen) aus.

   > **Note**
   >
   > Sie benötigen einen Snapshot Ihrer Datenbank, um damit arbeiten zu können. Wenn Sie noch keinen Snapshot erstellt haben, lesen Sie Erstellen eines Snapshots einer Datenbank.



6. Wählen Sie Create new database (Neue Datenbank erstellen) aus.
7. Wählen Sie auf der Seite Create a new database (Eine neue Datenbank erstellen) die Option Change zone (Zone ändern) aus, um eine andere Availablity Zone auszuwählen. Ihre neue Datenbank wird in der AWS-Region erstellt, in der sich der zuvor ausgewählte Snapshot befindet.
8. Wählen Sie Ihren neuen Datenbankplan aus.

   Wählen Sie einen Hochverfügbarkeits- oder einen Standard-Datenbankplan aus. Eine mit einem Hochverfügbarkeitsplan erstellte Datenbank verfügt über eine primäre Datenbank und eine sekundäre Standby-Datenbank in einer anderen Availability Zone für die Failover-Unterstützung. Weitere Informationen finden Sie unter Hochverfügbarkeitsdatenbanken.

> **Note**
>
> Sie können keinen Datenbankplan auswählen, der kleiner als der Plan der ursprünglichen Datenbank ist, mit der der Snapshot erstellt wurde.

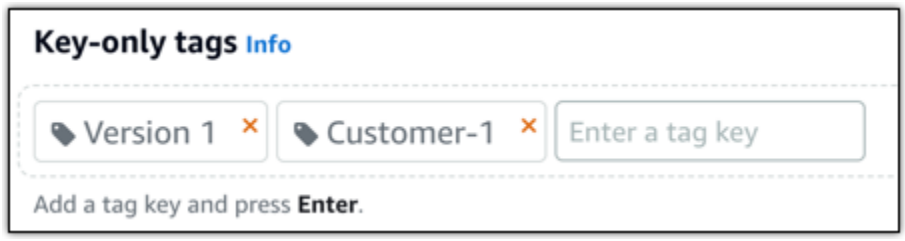
9. Geben Sie einen Namen für Ihre Datenbank ein.

   Ressourcennamen:

   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

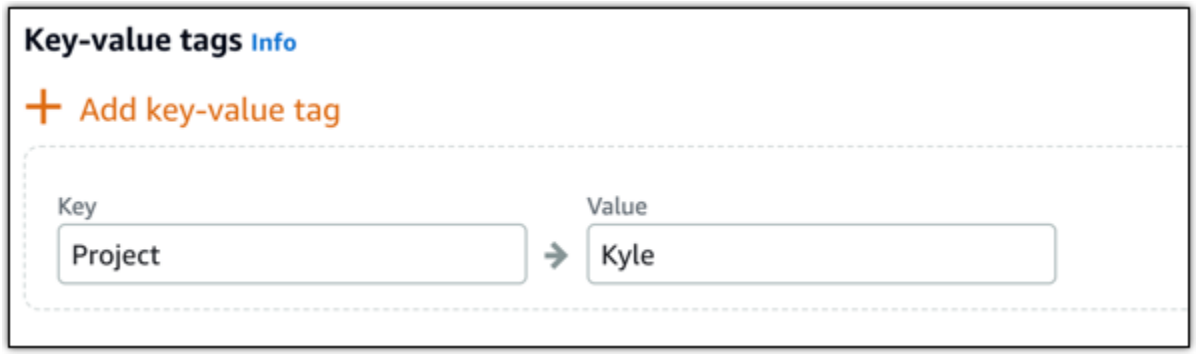
10. Wählen Sie eine der folgenden Optionen aus, um Ihrer Datenbank Tags hinzuzufügen:

    - Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.

    - Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

      Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.



> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

11. Wählen Sie Datenbank erstellen aus.

    Innerhalb weniger Minuten ist Ihre neue Lightsail-Datenbank mit dem neuen Datenbankplan oder -paket fertig.

Nächste Schritte

Führen Sie die folgenden Aktionen durch, nachdem Ihre neue Datenbank in Betrieb genommen wurde:

- Wenn Sie eine neue Datenbank erstellen, um eine bestehende Datenbank zu ersetzen, und wenn Sie eine Anwendung nutzen, die von der bestehenden Datenbank abhängig ist, stellen Sie sicher, dass Sie Ihre Anwendungsabhängigkeiten auf Ihre neue Datenbank aktualisieren.
- Löschen Sie die Originaldatenbank, wenn Sie sie nicht mehr benötigen. Weitere Informationen finden Sie unter Löschen Ihrer Datenbank.
- Datenbanken, die aus einem Snapshot erstellt wurden, sind so konfiguriert, dass sie ein von Lightsail erstelltes sicheres Passwort verwenden. Weitere Informationen finden Sie unter Verwaltung Ihres Datenbankpassworts.

Herunterladen eines SSL-Zertifikats für Ihre verwaltete Datenbank in Lightsail

Sie können Secure Socket Layer (SSL) oder Transport Layer Security (TLS) aus Ihrer Anwendung verwenden, um eine Verbindung zu einer verwalteten Datenbank in Amazon Lightsail mit MySQL oder PostgreSQL zu verschlüsseln. Jede DB-Engine hat einen eigenen Vorgang für die Implementierung von SSL/TLS. Weitere Informationen finden Sie unter Verwenden von SSL zum Herstellen einer Verbindung mit Ihrer MySQL-Datenbank oder Verwenden von SSL zum Herstellen einer Verbindung mit Ihrer PostgreSQL-Datenbank.

> **Note**
>
> Die zum Download verfügbaren Zertifikate sind mit Amazon Relational Database Service (Amazon RDS) gekennzeichnet, funktionieren aber auch für verwaltete Datenbanken in Lightsail.

Zertifikat-Pakete für alle AWS-Regionen

Um ein Zertifikatspaket zu erhalten, das sowohl Zwischen- als auch Stammzertifikate für alle AWS-Regionen enthält, oder wenn Ihre Anwendung unter Microsoft Windows läuft und eine PKCS7-Datei erfordert, finden Sie unter Zertifikatspakete für alle AWS-Regionen im Benutzerhandbuch für Amazon Relational Database Service weitere Informationen.

Dieses Stammzertifikat ist eine vertrauenswürdige Stammentität und sollte in den meisten Fällen funktionieren. Es könnte jedoch fehlschlagen, wenn Ihre Anwendung keine Zertifikatsketten akzeptiert. Fahren Sie mit dem nächsten Abschnitt dieses Dokuments fort, wenn Ihre Anwendung keine Zertifikatsketten akzeptiert.

Zertifikat-Pakete für bestimmte AWS-Regionen

Um ein Zertifikatspaket zu erhalten, das sowohl Zwischen- als auch Rootzertifikate für eine bestimmt AWS-Region enthält, finden Sie unter Zertifikatspakete für bestimmte AWS-Regionen im Benutzerhandbuch für Amazon Relational Database Service weitere Informationen.

Aktualisieren der Version des CA-Zertifikats für Ihre Lightsail-Datenbank

Amazon Lightsail hat neue Certificate Authority (CA)-Zertifikate für die Verbindung mit Ihrer verwalteten Datenbank mithilfe von SSL/TLS veröffentlicht. In diesem Handbuch wird beschrieben, wie Sie auf das neue CA-Zertifikat aktualisieren. Sie können das Zertifikat nur mithilfe der update-relational-database-API-Aktion aktualisieren. Die neuen Zertifikate werden als `rds-ca-rsa2048-g1`, `rds-ca-rsa4096-g1`und bezeichnet`rds-ca-ecc384-g1`. Das alte Zertifikat wird als bezeichnet`rds-ca-2019`. Als bewährte Methode für die - AWS Sicherheit stellen wir die CA-Zertifikate zur Verfügung. Informationen zu den CA-Zertifikaten für Ihre verwaltete Datenbank und den AWS-Regionen unterstützten finden Sie unter Herunterladen eines SSL-Zertifikats für Ihre verwaltete Datenbank.

Das alte CA-Zertifikat (`rds-ca-2019`) läuft am 22. August 2024 ab. Daher empfehlen wir dringend, die Schritte in diesem Handbuch so schnell wie möglich durchzuführen, um Ihre verwaltete Datenbank so zu ändern, dass das neue Zertifikat verwendet wird. Wenn Ihre Anwendungen keine Verbindung zu Ihrer von Lightsail verwalteten Datenbank über SSL/TLS herstellen, ist keine Aktion erforderlich. Wenn diese Schritte nicht abgeschlossen sind, können Ihre Anwendungen nach dem 22. August 2024 keine Verbindung mit Ihrer verwalteten Datenbank über SSL/TLS herstellen.

Neue verwaltete Datenbanken, die nach dem 26. Januar 2024 erstellt wurden, verwenden das `rds-ca-rsa2048-g1` Zertifikat standardmäßig. Wenn Sie neue verwaltete Datenbanken vorübergehend ändern möchten, um das alte Zertifikat (`rds-ca-2019`) zu verwenden, können Sie dies über die AWS Command Line Interface () tun AWS CLI. Alle verwalteten Datenbanken, die vor dem 26. Januar 2024 erstellt wurden`rds-ca-rsa2048-g1`, verwenden das `rds-ca-2019` Zertifikat, bis Sie sie auf die Zertifikate `rds-ca-rsa4096-g1`, und aktualisieren`rds-ca-ecc384-g1`.

> **Note**
>
> Testen Sie die Schritte in diesem Handbuch in einer Entwicklungs- oder Staging.Umgebung, bevor Sie diese in Produktionsumgebungen verwenden.

Voraussetzungen

- In diesem Handbuch verwenden Sie , AWS CloudShell um das Upgrade durchzuführen. CloudShell ist eine browserbasierte, vorauthentifizierte Shell, die Sie direkt über die Lightsail-Konsole starten können. Mit können CloudShellSie AWS Command Line Interface (AWS CLI)-Befehle

mit Ihrer bevorzugten Shell ausführen, z. B. Bash PowerShelloder Z-Shell. Sie können dies tun, ohne Befehlszeilentools herunterladen oder installieren zu müssen. Weitere Informationen zum Einrichten und Verwenden von finden Sie CloudShellunter AWS CloudShell in Lightsail .

- Bevor Sie die folgenden Schritte ausführen, müssen Sie die Datenbankanwendungen aktualisieren, um das neue SSL/TLS-Zertifikat zu verwenden. Die Methoden zur Aktualisierung von Anwendungen für neue SSL/TLS-Zertifikate hängen von Ihren spezifischen Anwendungen ab. Arbeiten Sie mit Ihren Anwendungsentwicklern zusammen, um die SSL/TLS-Zertifikate für Ihre Anwendungen zu aktualisieren. Weitere Informationen zum Aktualisieren von Anwendungen für neue SSL/TLS-Zertifikate finden Sie unter Aktualisieren von Anwendungen zur Verbindung mit MySQL-DB-Instances mit neuen SSL/TLS-Zertifikaten oder Aktualisieren von Anwendungen zur Verbindung mit PostgreSQL-DB-Instances mit neuen SSL/TLS-Zertifikaten im Benutzerhandbuch für Amazon Relational Database Service.

Identifizieren des aktiven CA-Zertifikats für Ihre verwaltete Datenbank

Führen Sie die folgenden Schritte aus, um das aktive CA-Zertifikat für Ihre Lightsail-Datenbank-Instance zu identifizieren.

1. Öffnen Sie ein TerminalAWS CloudShell-, - oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um das aktive CA-Zertifikat für Ihre verwaltete Datenbank zu identifizieren.

   ```
   aws lightsail get-relational-database --relational-database-name DatabaseName --
   region DatabaseRegion | grep "caCertificateIdentifier"
   ```

   Ersetzen Sie im Befehl durch *DatabaseName* den Namen der Datenbank, die Sie ändern möchten, und *DatabaseRegion* durch die , in der AWS-Region sich die Datenbank-Instance befindet.

   Beispiel

   ```
   aws lightsail get-relational-database --relational-database-name Database-1 --
   region us-east-1 | grep "caCertificateIdentifier"
   ```

   Der Befehl gibt die ID des aktiven CA-Zertifikats für Ihre Datenbank zurück.

   Beispiel

```
"caCertificateIdentifier": "rds-ca-rsa2048-g1"
```

Ändern der verwalteten Datenbank zur Verwendung des neuen Zertifizierungsstellenzertifikats

Führen Sie die folgenden Schritte aus, um Ihre verwaltete Datenbank in Lightsail so zu ändern`rds-ca-rsa2048-g1`, dass eines der neuen CA-Zertifikate (`rds-ca-rsa4096-g1`, und `rds-ca-ecc384-g1`) verwendet wird.

1. Öffnen Sie ein TerminalAWS CloudShell-, - oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um das neue Zertifikat in Ihrer verwalteten Datenbank zu verwenden.

   ```
   aws lightsail update-relational-database --relational-database-name DatabaseName --ca-certificate-identifier rds-ca-rsa2048-g1
   ```

   Ersetzen Sie im Befehl durch *`DatabaseName`* den Namen der Datenbank, die Sie ändern möchten.

   Beispiel

   ```
   aws lightsail update-relational-database --relational-database-name Database-1 --ca-certificate-identifier rds-ca-rsa2048-g1
   ```

   Das von Ihrer verwalteten Datenbank verwendete CA-Zertifikat wird während des nächsten Wartungsfensters Ihrer Datenbank oder sofort aktualisiert, wenn Sie den `--apply-immediately` Parameter am Ende des Befehls hinzufügen.

Ändern der verwalteten Datenbank zur Verwendung des alten Zertifizierungsstellenzertifikats

Führen Sie die folgenden Schritte aus, um Ihre verwaltete Datenbank in Lightsail so zu ändern, dass das alte CA-Zertifikat (`rds-ca-2019`) verwendet wird. Tun Sie dies nur`rds-ca-rsa4096-g1`, wenn Sie ein kritisches Problem mit einem der neuen Zertifikate (`rds-ca-rsa2048-g1`, und `rds-ca-ecc384-g1`) haben und das alte vorübergehend zurücksetzen müssen.

1. Öffnen Sie ein TerminalAWS CloudShell-, - oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um das `rds-ca-2019` in der verwalteten Datenbank zu verwenden.

   ```
   aws lightsail update-relational-database --relational-database-name DatabaseName --
   ca-certificate-identifier rds-ca-2019
   ```

   Ersetzen Sie im Befehl durch *`DatabaseName`* den Namen der Datenbank, die Sie ändern möchten.

   Beispiel

   ```
   aws lightsail update-relational-database --relational-database-name Database-1 --
   ca-certificate-identifier rds-ca-2019
   ```

   Das von Ihrer verwalteten Datenbank verwendete CA-Zertifikat wird während des nächsten Wartungsfensters Ihrer Datenbank oder sofort aktualisiert, wenn Sie den `--apply-immediately` Parameter am Ende des Befehls hinzufügen.

Ändern der bevorzugten Wartungs- und Sicherungsfenster für Ihre Lightsail-Datenbank

Wenn eine neue Version einer Datenbank von Amazon Lightsail unterstützt wird, kann Ihre bestehende verwaltete Datenbank auf diese aktualisiert werden. Es gibt zwei Arten von Upgrades – Minor-Versionsupgrades und Major-Versionsupgrades. Derzeit unterstützt Lightsail nur Minor-Versionsupgrades.

Minor-Versionsupgrades und andere Aufgaben der Datenbankpflege werden automatisch während des bevorzugten Wartungsfensters für Ihre Datenbank durchgeführt. Das bevorzugte Wartungsfenster ist ein 30-Minuten-Fenster, das nach dem Zufallsprinzip aus einem 8-Stunden-Zeitblock für jede AWS-Region ausgewählt wird. Es fällt auf einen zufälligen Wochentag. Datenbanksicherungen werden während des bevorzugten Sicherungsfensters durchgeführt. Das bevorzugte Sicherungsfenster ist ein 30-Minuten-Fenster, das nach dem Zufallsprinzip aus einem 8-Stunden-Zeitblock für jede AWS-Region ausgewählt wird. Es fällt ebenfalls auf einen zufälligen Wochentag.

> **Note**
>
> Weitere Informationen zu den bevorzugten Zeitblöcken für Wartungsfenster für jede Region finden Sie im Leitfaden Warten einer DB-Instance in der Dokumentation zum Amazon Relational Database Service (Amazon RDS). Weitere Informationen zu den bevorzugten Zeitblöcken für die Sicherungsfenster für jede Region finden Sie im Handbuch Arbeiten mit Sicherungen in der Amazon RDS-Dokumentation.

In diesem Handbuch erfahren Sie, wie Sie die bevorzugten Wartungs- und Sicherungsfenster so ändern, dass sie auftreten, wenn Ihre Datenbank unter der geringsten Last steht.

Voraussetzungen

Sie müssen die AWS Command Line Interface (AWS CLI) verwenden, um die von der Datenbank bevorzugten Wartungs- und Sicherungsfenster zu ändern.

Sie müssen folgende Voraussetzungen erfüllen:

- Installieren der AWS CLI – Weitere Informationen finden Sie unter Installieren der AWS CLI.
- Konfigurieren der AWS CLI – Weitere Informationen finden Sie unter Konfigurieren der AWS CLI.

Ändern des Fensters für die Datenbankwartung

Ihre Datenbank kann während Wartungs- oder Sicherungsarbeiten nicht mehr verfügbar sein. Daher können Sie Ihr bevorzugtes Wartungs- oder Sicherungsfenster auf einen Zeitpunkt ändern, an dem Ihre Datenbank unter der geringsten Last steht.

So ändern Sie das Fenster für die Datenbankwartung

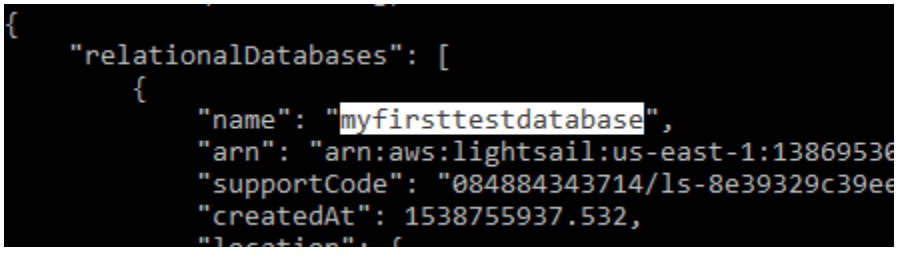
1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um den Namen der Datenbank zu erhalten, für die Sie das Wartungsfenster ändern möchten:

   ```
   aws lightsail get-relational-databases
   ```

   Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

> **Note**
>
> Wenn die Datenbank, die Sie ändern möchten, nicht aufgeführt ist, vergewissern Sie sich, dass Ihre AWS CLI für die AWS-Region konfiguriert ist, in der sich die Datenbank befindet. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI.

3. Markieren Sie den Namen der Datenbank, die Sie ändern möchten, und drücken Sie Strg+C, wenn Sie Windows verwenden, oder Cmd+C, wenn Sie macOS verwenden, um sie in Ihre Zwischenablage zu kopieren, damit Sie sie im nächsten Schritt verwenden können.



4. Geben Sie je nach dem bevorzugten Fenster, das Sie ändern, einen der folgenden Befehle ein.

- Geben Sie den folgenden Befehl ein, um das Datenbankverwaltungsfenster zu ändern.

```
aws lightsail update-relational-database --relational-database-name DatabaseName
 --preferred-maintenance-window MaintenanceWindow
```

Ersetzen Sie im Befehl Folgendes:

- *DatabaseName* durch den Namen der Datenbank.
- *MaintenanceWindow* durch den neuen Zeitrahmen des Wartungsfensters.

  Definieren Sie den bevorzugten Wartungsfensterzeitraum im Format ttt:hh24:mm-ttt:hh24:mm. Es muss außerdem im Universal Coordinated Time (UTC)-Format vorliegen und für ein Mindestfenster von 30 Minuten definiert sein. Das bevorzugte Wartungsfenster darf sich nicht mit dem bevorzugten Sicherungsfenster überschneiden.

Beispiel:

```
aws lightsail update-relational-database --relational-database-
name myproductiondb --preferred-maintenance-window Tue:16:00-Tue:16:30
```

- Geben Sie den folgenden Befehl ein, um das Datenbanksicherungsfenster zu ändern.

```
aws lightsail update-relational-database --relational-database-name DatabaseName
 --preferred-backup-window BackupWindow
```

Ersetzen Sie im Befehl Folgendes:

- *DatabaseName* durch den Namen der Datenbank.
- *BackupWindow* durch den neuen Zeitrahmen für das Sicherungsfenster.

  Definieren Sie das bevorzugte Sicherungszeitfenster im Format hh24:mm-hh24:mm. Es muss außerdem im Universal Coordinated Time (UTC)-Format vorliegen und für ein Mindestfenster von 30 Minuten definiert sein. Das bevorzugte Sicherungsfenster darf sich nicht mit dem bevorzugten Wartungsfenster überschneiden.

Beispiel:

```
aws lightsail update-relational-database --relational-database-
name myproductiondb --preferred-backup-window 14:00-14:30
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

Nächste Schritte

Hier sind ein paar Anleitungen, die Ihnen helfen, Ihre Datenbank zu verwalten:

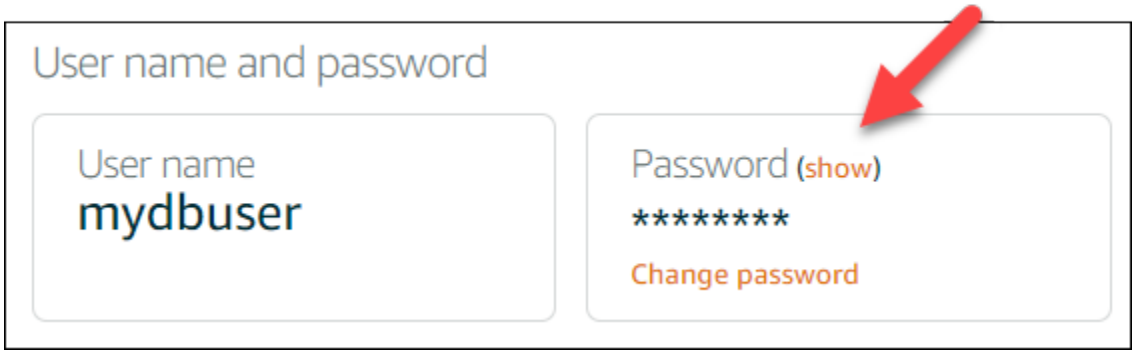
- Konfigurieren des Datenimportmodus für Ihre Datenbank
- Konfigurieren des öffentlichen Modus für Ihre Datenbank
- Verwalten Ihres Datenbankpassworts
- Verbinden mit Ihrer MySQL-Datenbank
- Herstellen einer Verbindung zu Ihrer PostgreSQL-Datenbank
- Importieren von Daten in Ihre MySQL-Datenbank
- Importieren von Daten in Ihre PostgreSQL-Datenbank
- Einen Snapshot Ihrer Datenbank erstellen

Verwalten Ihres Lightsail-Datenbankpassworts

Wenn Sie eine neue Datenbank in Amazon Lightsail erstellen, kann Lightsail für Sie ein sicheres Passwort erstellen, oder Sie können Ihr eigenes angeben. Das aktuelle Datenbankpasswort können Sie jederzeit in der Lightsail-Konsole einsehen oder ändern.

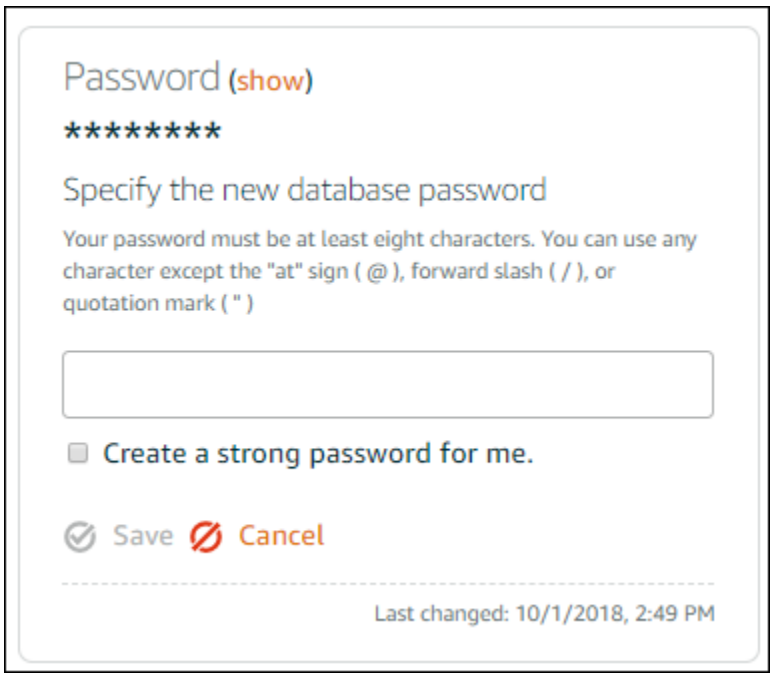
So verwalten Sie Ihr Datenbankpasswort

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Databases (Datenbanken) aus.
3. Wählen Sie den Namen der Datenbank, für die Sie das Passwort verwalten möchten.
4. Wählen Sie auf der Registerkarte Connect (Verbinden) unter dem Abschnitt User name and passwords (Benutzername und Passwörter) die Option Show (Anzeigen), um das aktuelle Datenbankpasswort anzuzeigen.



5. Um das Datenbankpasswort zu ändern, wählen Sie Change password (Passwort ändern).

   Sie können sich dafür entscheiden, dass Lightsail ein starkes Passwort für Sie erstellt, oder Sie können Ihr eigenes Passwort in das Textfeld eingeben. Das Passwort kann jedes druckbare ASCII-Zeichen mit Ausnahme von "/", """ oder "@" enthalten. Für MySQL-Datenbanken muss das Passwort zwischen 8 und 41 Zeichen enthalten. Für PostgreSQL-Datenbanken muss das Passwort zwischen 8 und 128 Zeichen enthalten.



6. Klicken Sie auf Save (Speichern), wenn Sie damit fertig sind.

   Eine Änderung des Datenbankpassworts wird sofort wirksam. Wenn Sie Ihr eigenes Passwort eingegeben haben, wird das Passwort sofort gespeichert. Wenn Lightsail das Passwort für Sie erstellt, wird es innerhalb weniger Sekunden generiert. Wählen Sie Show (Anzeigen) um das neue Passwort anzuzeigen.

Nächste Schritte

Hier sind ein paar Anleitungen, die Ihnen helfen, Ihre Datenbank in Lightsail zu verwalten:

- Verbinden mit Ihrer MySQL-Datenbank
- Herstellen einer Verbindung zu Ihrer PostgreSQL-Datenbank
- Einen Snapshot Ihrer Datenbank erstellen

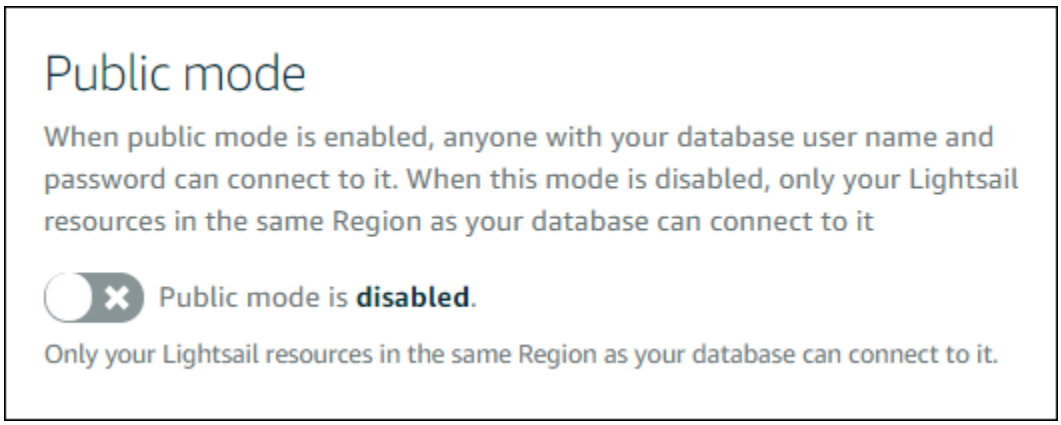
Konfigurieren des öffentlichen Modus für Ihre Lightsail-Datenbank

Ihre verwaltete Datenbank in Amazon Lightsail ist nur für Ihre Lightsail-Ressourcen (Instances, Load Balancer etc.) zugänglich, die sich im selben Lightsail-Konto befinden. Ein häufiges Szenario ist es, sowohl eine Lightsail-Instance mit einer öffentlich zugänglichen Webanwendung als auch eine Lightsail-Datenbank, die nicht öffentlich zugänglich ist, zu erstellen und diese dann zu verbinden.

Aktivieren Sie die Feature für den öffentlichen Modus, um Ihre Datenbank öffentlich zugänglich zu machen. Auf diese Weise kann sich jeder mit Datenbank-Endpunkt, Port, Benutzername und Passwort mit Ihrer Datenbank verbinden. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer MySQL-Datenbank oder Herstellen einer Verbindung zu Ihrer PostgreSQL-Datenbank.

So konfigurieren Sie den öffentlichen Modus für Ihre Datenbank:

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Databases (Datenbanken) aus.
3. Wählen Sie den Namen der Datenbank aus, für die Sie den öffentliche Modus konfigurieren möchten.
4. Wählen Sie die Registerkarte Network (Network) aus.
5. Verwenden Sie unter dem Abschnitt Public mode (Öffentlicher Modus) den Schalter, um ihn einzuschalten. Mit dem Schalter können Sie ihn auch wieder ausschalten.



   Die Einstellung für die öffentliche Zugänglichkeit wird sofort aktiv. Der Abschluss der Umstellung kann aber einige Minuten in Anspruch nehmen. Während dieser Zeit ändert sich der Status Ihrer Datenbank auf Modifying (Ändern). Der Status Ihrer Datenbank ändert sich auf Available (Verfügbar), nachdem die Einstellung für die öffentliche Zugänglichkeit angewendet wurde.

Nächste Schritte

Hier sind ein paar Anleitungen, die Ihnen helfen, Ihre Datenbank zu verwalten:

- Konfigurieren des Datenimportmodus für Ihre Datenbank
- Verwalten Ihres Datenbankpassworts

- Verbinden mit Ihrer MySQL-Datenbank
- Herstellen einer Verbindung zu Ihrer PostgreSQL-Datenbank
- Importieren von Daten in Ihre MySQL-Datenbank
- Importieren von Daten in Ihre PostgreSQL-Datenbank
- Einen Snapshot Ihrer Datenbank erstellen

Aktualisieren von Lightsail-Datenbank-Parametern

Database Parameter, auch bekannt als Datenbank-Systemvariablen, definieren die grundlegenden Eigenschaften einer verwalteten Datenbank in Amazon Lightsail. Sie können beispielsweise einen Datenbankparameter definieren, um die Anzahl der Datenbankverbindungen zu begrenzen, oder einen anderen Parameter, um die Größe des Datenbankpufferpools zu begrenzen. In dieser Anleitung lernen Sie, wie Sie eine Liste der Parameter für Ihre verwaltete Datenbank erhalten und wie Sie diese mit Hilfe von AWS Command Line Interface (AWS CLI) aktualisieren können.

> **Note**
>
> Weitere Informationen zu MySQL-Systemvariablen finden Sie in der MySQL 5.6-, MySQL 5.7- oder MySQL 8.0-Dokumentation. Weitere Informationen zu PostgreSQL-Systemvariablen finden Sie in der PostgreSQL 9.6-, PostgreSQL 10-, PostgreSQL 11- oder PostgreSQL 12-Dokumentation.

Voraussetzungen

- Falls noch nicht erfolgt, installieren und konfigurieren Sie die AWS CLI. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

Eine Liste der verfügbaren Datenbankparameter abrufen

Die Datenbankparameter unterscheiden sich je nach Datenbank-Engine. Aus diesem Grund sollten Sie eine Liste der verfügbaren Parameter für Ihre verwaltete Datenbank abrufen. Auf diese Weise können Sie entscheiden, welche Parameter Sie ändern möchten, und die Art und Weise, wie dieser Parameter wirksam werden.

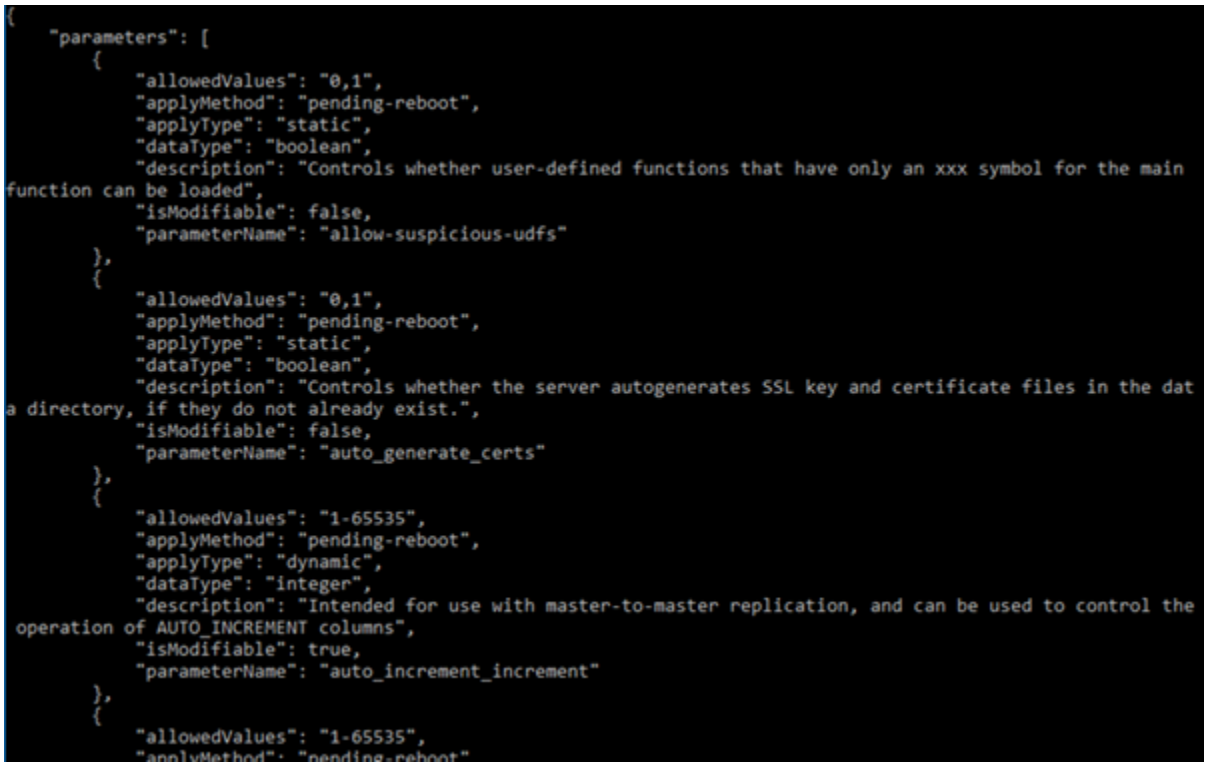
Um eine Liste der verfügbaren Datenbankparameter abzurufen

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um eine Liste der Parameter für Ihre Datenbank abzurufen.

```
aws lightsail get-relational-database-parameters --relational-database-
name DatabaseName
```

Ersetzen Sie im Befehl *DatabaseName* durch den Namen Ihrer Datenbank.

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:



> **Note**
>
> Wenn die Parameterergebnisse paginiert sind, wird eine nächste Seite der Token-IDs aufgelistet. Notieren Sie sich die Token-ID der nächsten Seite und verwenden Sie sie wie im nächsten Schritt gezeigt, um die nächste Seite der Parameterergebnisse anzuzeigen.

3. Wenn Ihre Ergebnisse paginiert sind, verwenden Sie den folgenden Befehl, um den zusätzlichen Satz von Parametern anzuzeigen. Andernfalls überspringen Sie diesen Schritt und gehen Sie direkt zum nächsten.

```
aws lightsail get-relational-database-parameters --relational-database-
name DatabaseName --page-token NextPageTokenID
```

Ersetzen Sie im Befehl Folgendes:

- *DatabaseName* durch den Namen Ihrer Datenbank.
- *NextPageTokenID* durch die Token-ID der nächsten Seite.

Das Ergebnis zeigt für jeden Datenbankparameter die folgenden Informationen an:

- Allowed values – gibt den gültigen Wertbereich für den Parameter an.
- Apply method – gibt an, wann die Parameteränderung angewendet wird. Erlaubte Optionen sind `immediate` oder `pending-reboot`. Weitere Informationen zur Festlegung der Anwendungsmethode finden Sie im folgenden Anwendungstyp.
- Apply type – gibt die Engine-spezifische Art der Übergabe an. Wenn `dynamic` aufgeführt ist, kann der Parameter mit einer `immediate`-apply-Methode angewendet werden und die Datenbank beginnt sofort mit dem neuen Parameterwert. Wenn `static` aufgeführt ist, kann der Parameter nur mit einer `pending-reboot`-apply-Methode angewendet werden und die Datenbank beginnt erst nach ihrem Neustart mit dem neuen Parameterwert.
- Data type – gibt den gültigen Datentyp für den Parameter an.
- Description – liefert eine Beschreibung des Parameters.
- Is modifiable – ist ein Boolescher Wert, der angibt, ob der Parameter geändert werden kann. Wenn `true` angegeben ist, kann der Parameter geändert werden.
- Parameter name – gibt den Namen des Parameters an. Verwenden Sie diesen Wert zusammen mit der `update relational database`-Operation und dem `parameter name`-Parameter.

4. Suchen Sie den Parameter, den Sie ändern möchten, und notieren Sie sich den Parameternamen, die zulässigen Werte und die Apply-Methode. Wir empfehlen, den Parameternamen in die Zwischenablage zu kopieren, um eine falsche Eingabe zu vermeiden. Markieren Sie dazu den Parameternamen und drücken Sie Ctrl+C (Strg+C), wenn Sie Windows verwenden, oder Cmd+C, wenn Sie macOS verwenden, um ihn in die Zwischenablage zu kopieren. Drücken Sie dann Strg+V oder Cmd+V, um ihn einzufügen.

Nachdem Sie den Namen des zu ändernden Parameters identifiziert haben, fahren Sie mit dem nächsten Abschnitt dieser Anleitung fort, um den Parameter auf den von Ihnen gewünschten Wert zu ändern.

Aktualisieren Sie Ihre Datenbankparameter

Nachdem Sie den Namen des zu ändernden Parameters festgelegt haben, führen Sie die folgenden Schritte aus, um den Parameter für Ihre verwaltete Datenbank in Lightsail zu ändern:

Um Ihre Datenbankparameter zu aktualisieren

- Geben Sie den folgenden Befehl in ein Terminal- oder Befehlszeilenfenster zum Aktualisieren eines Parameters für Ihre verwaltete Datenbank ein.

```
aws lightsail update-relational-database-parameters
 --relational-database-name DatabaseName --parameters
 "parameterName=ParameterName,parameterValue=NewParameterValue,applyMethod=ApplyMethod"
```

Ersetzen Sie im Befehl Folgendes:

- *DatabaseName* durch den Namen Ihrer Datenbank.
- *ParameterName* durch den Namen des Parameters, den Sie ändern möchten.
- *NewParameterValue* durch den neuen Wert des Parameters.
- *ApplyMethod* durch die Anwendungsmethode für den Parameter.

  Wenn der Anwendungstyp des Parameters `dynamic` ist, kann der Parameter mit einer `immediate`-apply-Methode angewendet werden und die Datenbank beginnt sofort mit dem neuen Parameterwert. Wenn jedoch der Anwendungstyp des Parameters `static` ist, kann der Parameter nur mit einer `pending-reboot`-apply-Methode angewendet werden und die Datenbank beginnt erst nach ihrem Neustart mit dem neuen Parameterwert.

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

Der Datenbankparameter wird in Abhängigkeit von der verwendeten Anwendungsmethode aktualisiert.

Aktualisieren der Hauptversion einer Lightsail-Datenbank

Wenn Amazon Lightsail eine neue Version einer Datenbank-Engine unterstützt, können Sie Ihre Datenbank auf die neue Version aktualisieren. Lightsail bietet zwei Datenbankvorlagen: MySQL und PostgreSQL . In diesem Handbuch wird beschrieben, wie Sie die Hauptversion für Ihre MySQL- oder PostgreSQL-Datenbank-Instance aktualisieren. Sie können die Hauptversion der Datenbank nur mithilfe der APIupdate-relational-database-Aktion aktualisieren.

Wir werden verwenden AWS CloudShell , um das Upgrade durchzuführen. CloudShell ist eine browserbasierte, vorauthentifizierte Shell, die Sie direkt über die Lightsail-Konsole starten können. Mit können CloudShellSie AWS Command Line Interface (AWS CLI)-Befehle mit Ihrer bevorzugten Shell ausführen, z. B. Bash PowerShelloder Z-Shell. Sie können dies tun, ohne Befehlszeilentools herunterladen oder installieren zu müssen. Weitere Informationen zum Einrichten und Verwenden von finden Sie CloudShellunter AWS CloudShell in Lightsail .

Die Änderungen verstehen

Hauptversions-Upgrades können zu einer Reihe von Inkompatibilitäten mit der vorherigen Version führen. Diese Inkompatibilitäten können während eines Upgrades zu Problemen führen. Möglicherweise müssen Sie Ihre Datenbank darauf vorbereiten, dass das Upgrade erfolgreich ist.

Weitere Informationen zum Aktualisieren von Hauptversionen einer Datenbank finden Sie in den folgenden Themen auf den MySQL- und PostgreSQL-Websites.

- Vorbereiten Ihrer Installation für das Upgrade
- MySQL Upgrade Checker Utility
- Aktualisieren eines PostgreSQL-Clusters

Voraussetzungen

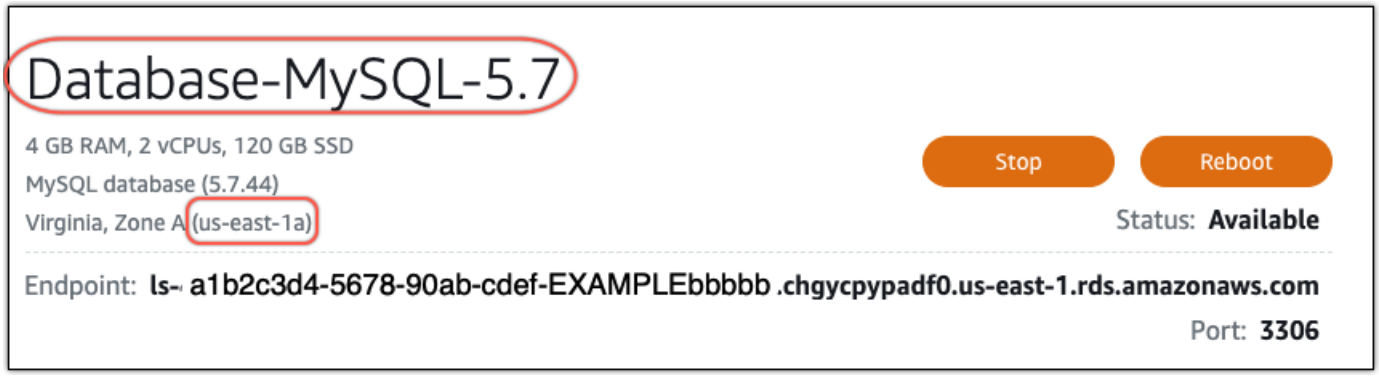
1. Stellen Sie sicher, dass Ihre Anwendung beide Hauptversionen der Datenbank unterstützt.
2. Wir empfehlen Ihnen, einen Snapshot Ihrer Datenbank-Instance zu erstellen, bevor Sie Änderungen vornehmen. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Lightsail-Datenbank.
3. (Optional) Erstellen Sie eine neue Datenbank-Instance aus dem Snapshot, den Sie gerade erstellt haben. Da Datenbankaktualisierungen Ausfallzeiten erfordern, können Sie das Upgrade auf der neuen Datenbank testen, bevor Sie die derzeit aktive Datenbank aktualisieren. Weitere Informationen zum Erstellen einer Kopie Ihrer Datenbank finden Sie unter Erstellen eines Snapshots Ihrer Lightsail-Datenbank.

Aktualisieren der Hauptversion der Datenbank

Lightsail unterstützt Hauptversions-Upgrades für MySQL- und PostgreSQL-Datenbank-Instances. Eine MySQL-Datenbank wird im folgenden Verfahren als Beispiel verwendet. Der Prozess und die Befehle sind jedoch für eine PostgreSQL-Datenbank identisch.

Führen Sie das folgende Verfahren aus, um die Hauptversion der Datenbank für Ihre Lightsail-Datenbank zu aktualisieren.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie im linken Navigationsbereich Datenbanken aus.
3. Notieren Sie sich den Namen und AWS-Region die für die Datenbank-Instance, die Sie aktualisieren möchten.



4. Wählen Sie in der unteren linken Ecke der Lightsail-Konsole ausCloudShell. Ein CloudShell Terminal wird auf derselben Browser-Registerkarte geöffnet. Wenn die Eingabeaufforderung angezeigt wird, ist die Shell für die Interaktion bereit.
5. Geben Sie in der CloudShell Eingabeaufforderung den folgenden Befehl ein, um eine Liste der verfügbaren Datenbank-Blueprint-IDs abzurufen.

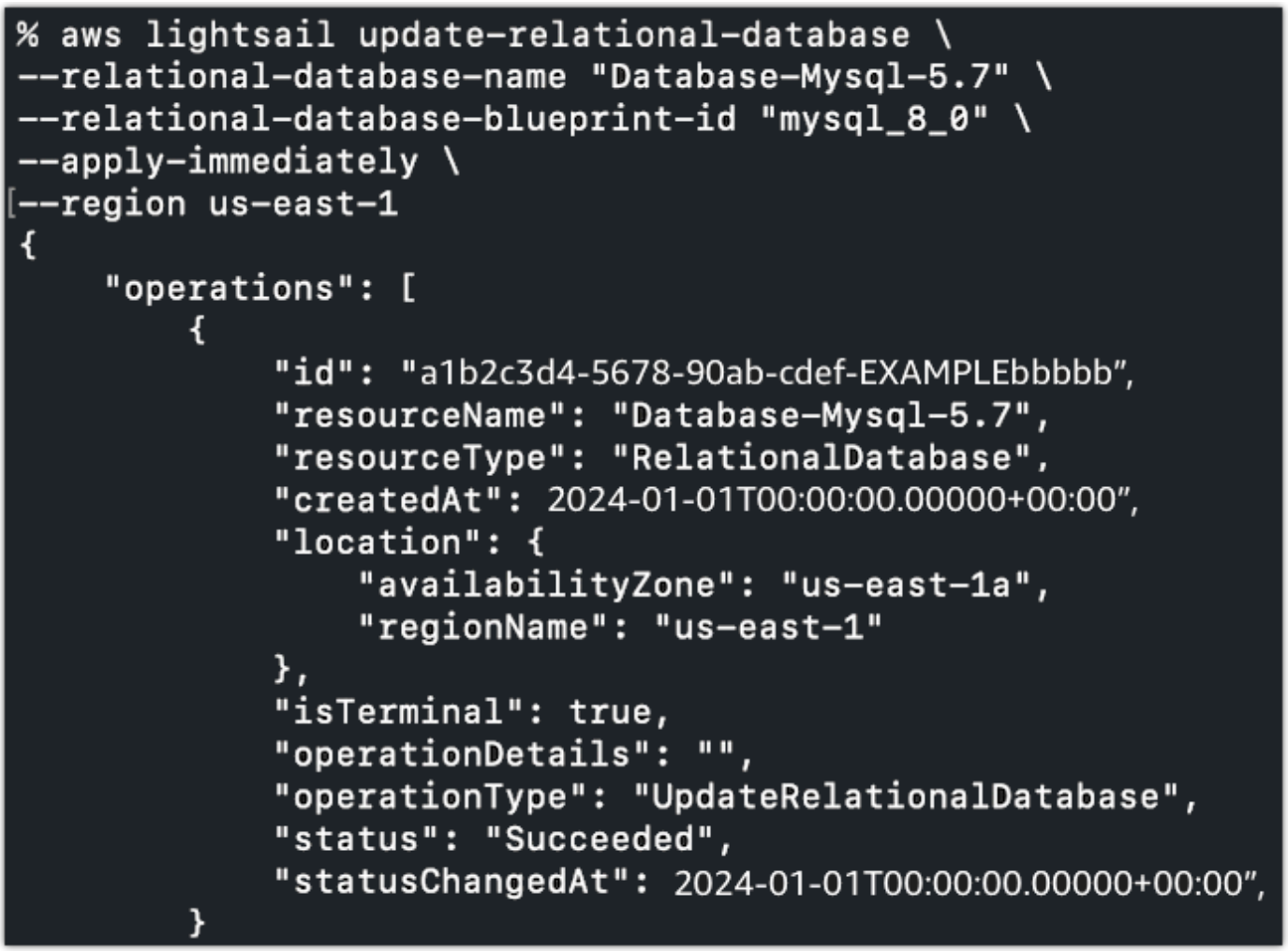
```
aws lightsail get-relational-database-blueprints
```

6. Notieren Sie sich die Blueprint-ID für die Hauptversion, auf die Sie aktualisieren. Beispiel: `mysql_8_0`

7. Geben Sie den folgenden Befehl ein, um die Hauptversion Ihrer Datenbank zu aktualisieren. Das Upgrade wird während des nächsten Wartungsfensters für Ihre Datenbank durchgeführt. Ersetzen Sie im Befehl durch *DatabaseName* den Namen Ihrer Datenbank, *blueprintId* durch die Blueprint-ID der Hauptversion, auf die Sie aktualisieren, und *DatabaseRegion* durch die AWS-Region , in der sich Ihre Datenbank befindet.

```
aws lightsail update-relational-database \
 --relational-database-name DatabaseName \
 --relational-database-blueprint-id blueprintId \
 --region DatabaseRegion
```

(Optional) Um das Upgrade sofort anzuwenden, fügen Sie den `--apply-immediately` Parameter in den Befehl ein. Es wird eine Antwort ähnlich dem folgenden Beispiel angezeigt, und Ihre Datenbank ist nicht mehr verfügbar, während das Upgrade angewendet wird. Weitere Informationen finden Sie unter update-relational-database in der Lightsail-API-Referenz.



8. Geben Sie den folgenden Befehl ein, um zu überprüfen, ob das Upgrade der Hauptversion für das nächste Datenbankwartungsfenster geplant ist. Ersetzen Sie im Befehl durch *DatabaseName* den Namen Ihrer Datenbank und *DatabaseRegion* durch die AWS-Region , in der sich Ihre Datenbank befindet.

```
aws lightsail get-relational-database \
 --relational-database-name DatabaseName \
 --region DatabaseRegion
```

In der `get-relational-database` Antwort state informiert Sie die Datenbank während des nächsten Wartungsfensters über ein ausstehendes Hauptversions-Upgrade. Datum und Uhrzeit des nächsten Wartungsfensters finden Sie im preferredMaintenanceWindow Abschnitt der Antwort.

Status der Datenbank-Instance

```
"state": "upgrading",
  "backupRetentionEnabled": true,
  "pendingModifiedValues": {
  "engineVersion": "8.0.36"
```

Wartungsfenster

```
"preferredMaintenanceWindow": "wed: 09:22-wed: 09:52"
```

Nächste Schritte

Wenn Sie eine Testdatenbank erstellt haben, können Sie sie löschen, nachdem Sie sich vergewissert haben, dass Ihre Anwendung mit der aktualisierten Datenbank funktioniert. Behalten Sie den Snapshot bei, den Sie für Ihre vorherige Datenbank erstellt haben, falls Sie zu ihr zurückkehren müssen. Sie sollten auch einen Snapshot Ihrer aktualisierten Datenbank erstellen, damit Sie eine neue point-in-time Kopie davon haben.

Loadbalancer in Amazon Lightsail

Ein Lightsail-Load Balancer verteilt eingehenden Web-Datenverkehr auf mehrere Lightsail-Instances in mehreren Availability Zones. Load Balancing erhöht die Verfügbarkeit und Fehlertoleranz der Anwendung auf Ihren Instances. Sie können Instances zu Ihrem Lightsail-Load Balancer hinzufügen und Instances entfernen, wenn sich Ihre Bedürfnisse ändern, ohne den allgemeinen Fluss von Anfragen an Ihre Anwendung zu unterbrechen.

Mit dem Lightsail-Lastausgleich erstellen wir einen DNS-Hostnamen und leiten alle Anforderungen, die an diesen Hostnamen gesendet werden, an einen Pool von Lightsail-Ziel-Instances weiter. Sie können Ihres Load Balancers beliebig viele Ziel-Instances hinzufügen, solange Sie Ihre Lightsail-Kontokontingente für die Gesamtanzahl der Instances nicht erschöpfen.

Feature des Load Balancers

Lightsail-Load Balancer bieten folgende Funktionen:

- HTTPS-Verschlüsselung – Standardmäßig verarbeiten Lightsail-Load Balancer unverschlüsselte Datenverkehrsanforderungen (HTTP) über Port 80. Aktivieren Sie die HTTPS-Verschlüsselung, indem Sie ein validiertes Lightsail-SSL-/TLS-Zertifikat an Ihren Load Balancer anfügen. Dies ermöglicht es dem Load Balancer, verschlüsselte (HTTPS-) Datenverkehrsanfragen über Port 443 zu verarbeiten. Weitere Informationen finden Sie unter SSL/TLS-Zertifikate.

  Die folgenden Funktionen stehen zur Verfügung, nachdem Sie die HTTPS-Verschlüsselung für Ihren Load Balancer aktiviert haben:

  - HTTP-zu-HTTPS-Umleitung – Aktivieren Sie die HTTP-zu-HTTPS-Umleitung, um HTTP-Anfragen automatisch an eine HTTPS-verschlüsselte Verbindung umzuleiten. Weitere Informationen finden Sie unter Konfigurieren der HTTP-zu-HTTPS-Umleitung für Ihren Load Balancer.
  - TLS-Sicherheitsrichtlinien – Konfigurieren Sie eine TLS-Sicherheitsrichtlinie für Ihren Load Balancer. Weitere Informationen finden Sie unter Konfigurieren von TLS-Sicherheitsrichtlinien auf Ihren Amazon Lightsail-Load Balancers.
- Zustandsprüfung – Standardmäßig werden Zustandsprüfungen auf den angefügten Instances im Root der Webanwendung durchgeführt, die auf ihnen ausgeführt wird. Die Zustandsprüfungen überwachen den Zustand der Ziel-Instances, sodass der Load Balancer nur Anfragen an fehlerfreie Instances senden kann. Weitere Informationen finden Sie unter Zustandsprüfung für einen Lightsail-Load Balancer.

- Sitzungspersistenz – Konfigurieren Sie die Sitzungspersistenz, wenn Sie Sitzungsinformationen lokal in den Browsern der Website-Besucher speichern. Sie könnten zum Beispiel eine Magento-E-Commerce-Anwendung mit einem Warenkorb auf Ihren Lightsail-Instances mit Lastausgleich betreiben. Wenn Ihre Website-Besucher Artikel in den Warenkorb legen und dann ihre Sitzung beenden, sind die Artikel im Warenkorb noch vorhanden, wenn sie zurückkommen, sofern Sie die Sitzungspersistenz konfiguriert haben. Weitere Informationen finden Sie unter Aktivieren der Sitzungspersistenz für einen Load Balancer.

Empfohlene Verwendung von Load Balancers

Verwenden Sie einen Load Balancer, wenn Ihre Website gelegentliche Datenverkehrsspitzen aufweist oder wenn Sie Inhalt hosten, der bei gleichzeitiger Nutzung durch viele Besucher zu hohen Lasten auf einer Instance führt. Wenn Sie zum Beispiel eine Website mit zahlreichen Images haben, kann für die Image-Anforderungen ein Lastenausgleich mit den anderen Seitenanfragen stattfinden. Auf diese Weise werden die Seiten schneller geladen und die Benutzerzufriedenheit steigt.

Sie können mit einem Load Balancer eine hochverfügbare Website erstellen. Hohe Verfügbarkeit bezieht sich darauf, wie lange die Website oder Anwendung innerhalb eines bestimmten Zeitraums verfügbar ist. Wenn die Website schon einmal ausgefallen ist, können Sie die Betriebsdauer durch einen Load Balancer erhöhen. Sie können einen Lightsail-Load Balancer verwenden, um Ihre Anwendung hoch verfügbar zu machen, indem Sie Ziel-Instances hinzufügen, die über mehrere Availability Zones verteilt sind.

Fehlertoleranz ist ein verwandtes Konzept. Wenn Ihre Website auch dann weiter funktioniert, wenn eine der Instances oder die Datenbank ausfällt, wird sie als tolerant betrachtet. Mit einem Load Balancer können Sie eine fehlertolerante Anwendung oder Website erstellen.

Empfohlene -Anwendungen für einen Lastenausgleich

Nicht alle Lightsail-Anwendungen erfordern Load Balancer. Wenn Sie eine Anwendung mit Lastenausgleich erstellen möchten, müssen Sie zuerst Ihre Anwendung konfigurieren. Um beispielsweise eine LAMP-Stack-Anwendung auf das Load Balancing vorzubereiten, sollten Sie zunächst eine zentrale, dedizierte Datenbank erstellen, aus der alle Ziel-Instances lesen und in die sie schreiben können. Sie könnten auch erwägen, zentralisierten Medienspeicher zu erstellen, z. B. einen Lightsail-Objektspeicher-Bucket. Weitere Informationen finden Sie unter Konfigurieren einer Instance für Load Balancing.

Erste Schritte mit einem Load Balancer

Zum Erstellen eines Load Balancers können Sie die Lightsail-Konsole, die AWS Command Line Interface (AWS CLI) oder die Lightsail-API verwenden. Außerdem ist das Konfigurieren der Instances für Load Balancing erforderlich.

Nachdem Sie den Load Balancer erstellt und die konfigurierten Instances angefügt haben, können Sie mithilfe des folgenden Themas HTTPS aktivieren. Weitere Informationen finden Sie unter Erstellen eines SSL-/TLS-Zertifikats für Ihren Load Balancer.

Erstellen eines Lightsail-Load-Balancers und Anfügen von Instances

Erstellen Sie einen -Load-Balancer, um Ihre Anwendung redundant zu gestalten oder um mehr Web-Datenverkehr zu bewältigen. Nachdem der Load Balancer erstellt wurde, können Sie die Lightsail-Instances anfügen, die Sie lastverteilen möchten. Weitere Informationen finden Sie unter Load Balancer

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie Ihre Lightsail-Instance für das Load-Balancing vorbereitet haben. Weitere Informationen finden Sie unter Konfigurieren einer Instance für Load Balancing.

Erstellen eines Load Balancers

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie die Registerkarte Network (Network) aus.
3. Wählen Sie Create load balancer (Load Balancer erstellen) aus.
4. Bestätigen Sie die AWS-Region, in der der Load Balancer erstellt wird, oder wählen Sie Region ändern, um eine andere Region auswählen.

> **Note**
>
> Standardmäßig wird der Load Balancer mit offenem Port 80 erstellt, um HTTP-Anfragen entgegenzunehmen. Nachdem der Load Balancer erstellt wurde, können Sie ein SSL/

TLS-Zertifikat erstellen und HTTPS konfigurieren. Weitere Informationen finden Sie unter Erstellen eines SSL-/TLS-Zertifikats für Ihren Load Balancer

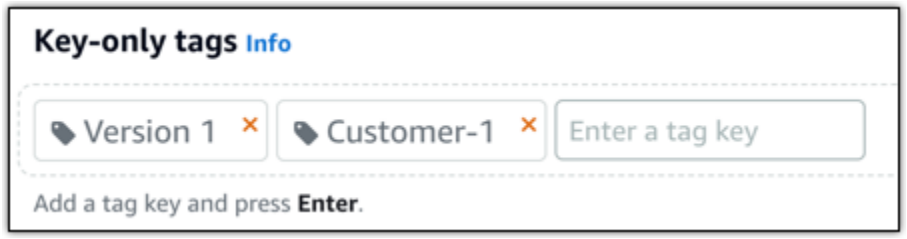
5. Geben Sie einen Namen für Ihren Load Balancer ein.

   Ressourcennamen:

   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

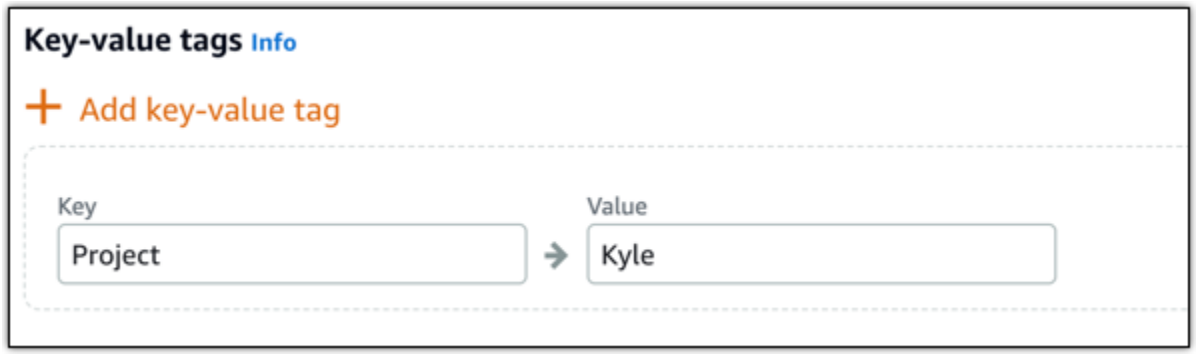
6. Wählen Sie eine der folgenden Optionen, um Ihrem Load Balancer Tags hinzuzufügen:

   - Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.

   - Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

     Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.



> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

7. Wählen Sie Create load balancer (Load Balancer erstellen) aus.

Anfügen von Instances an den Load Balancer

Nachdem Ihr Load Balancer erstellt wurde, führt Sie Lightsail auf die Verwaltungsseite des Load Balancers. Wenn Sie diese Seite wiederfinden möchten, wählen Sie die Registerkarte Networking (Netzwerk) auf der Lightsail-Startseite und wählen Sie dann den Namen Ihres Lightsail-Load-Balancers, um sie zu verwalten.

> **Note**
>
> Ihre Lightsail-Instance muss ausgeführt werden, bevor Sie sie erfolgreich an den Load Balancer anfügen können.

1. Wählen Sie auf der Verwaltungsseite für den Load Balancer Target instances (Ziel-Instances) aus.
2. Wählen Sie eine Instance im Dropdown-Menü Target instances (Ziel-Instances).
3. Wählen Sie Attach (Anfügen) aus. Das Zuweisen kann mehrere Minuten dauern.

   Fügen Sie eine andere Instance an den Load Balancer an, indem Sie Attach another (Andere anfügen) auswählen und dann die vorherigen Schritte wiederholen.

Nächste Schritte

Nachdem der Load Balancer erstellt und Ihre Instances angefügt wurden, führen Sie die folgenden Schritte aus, um Ihren Load Balancer zu konfigurieren:

- Erstellen eines SSL-/TLS-Zertifikats für Ihren Load Balancer
- Zustandsprüfungen für Ihren Load Balancer konfigurieren

Wenn Sie Probleme mit Ihrem Load Balancer haben, finden Sie Hilfe unter Fehlerbehebung bei Ihrem Load Balancer

Erstellen eines SSL-/TLS-Zertifikats für Ihren Amazon Lightsail-Load Balancer

Nach dem Erstellen eines Lightsail-Load Balancers können Sie ein Transport Layer Security (TLS)-Zertifikat anfügen, um HTTPS zu aktivieren. Dank des SSL-/TLS-Zertifikats kann Ihr Load Balancer verschlüsselten Web-Datenverkehr verarbeiten, sodass Sie Ihren Benutzern mehr Sicherheit bieten können. Weitere Informationen finden Sie unter SSL-/TLS-Zertifikate.

Voraussetzungen

Bevor Sie beginnen, benötigen Sie Folgendes.

- Ein Lightsail-Load Balancer. Weitere Informationen finden Sie unter Erstellen eines Load Balancers.

Erstellen der Zertifikatsanforderung

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Networking (Netzwerk).
3. Wählen Sie den Namen des Load Balancers, für die Sie ein SSL-/TLS-Zertifikat konfigurieren möchten.
4. Wählen Sie die Registerkarte Custom domains (Benutzerdefinierte Domains).
5. Wählen Sie Create certificate (Zertifikat erstellen).
6. Geben Sie einen Namen für Ihr Zertifikat ein oder übernehmen Sie die Standardeinstellung.

Ressourcennamen:

- Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
- Muss zwischen 2 und 255 Zeichen enthalten.
- Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
- Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

7. Geben Sie Ihre primäre Domain (`www.example.com`) und bis zu 9 alternative Domains oder Subdomains ein.

   Weitere Informationen finden Sie unter Hinzufügen von alternativen Domains und Subdomains zu Ihrem SSL-/TLS-Zertifikat.

8. Wählen Sie Create certificate (Zertifikat erstellen).

   Lightsail startet den Validierungsprozess. Sie haben 72 Stunden Zeit, um zu verifizieren, dass Sie Eigentümer der Domain sind.

   Nachdem Sie Ihr Zertifikat erstellt haben, wird es zusammen mit dem Domainnamen und allen alternativen Domains und Subdomains angezeigt. Sie müssen einen DNS-Datensatz für jede Domain und Subdomain erstellen.

Nächster Schritt

- Verifizieren, dass Sie Eigentümer der Domain sind

Themen

- Hinzufügen von alternativen Domains und Subdomains zu Ihrem SSL-/TLS-Zertifikat in Lightsail
- Überprüfen eines SSL-/TLS-Zertifikats in Amazon Lightsail
- Anfügen eines gültigen SSL-/TLS-Zertifikats an den Amazon Lightsail-Load Balancer
- Löschen eines SSL/TLS-Zertifikats in Amazon Lightsail

Hinzufügen von alternativen Domains und Subdomains zu Ihrem SSL-/TLS-Zertifikat in Lightsail

Wenn Sie das SSL-/TLS-Zertifikat für den Lightsail-Load Balancer erstellen, können Sie ihm alternative Domains und Subdomains hinzufügen. Mit diesen alternativen Namen wird sichergestellt, dass der gesamte Datenverkehr an den Load Balancer verschlüsselt ist.

Wenn Sie eine primäre Domain angeben, können Sie einen vollständig qualifizierten Domainnamen wie `www.example.com` oder einen Apex-Domainnamen wie beispielsweise `example.com` verwenden.

Die Gesamtzahl der Domains und Subdomains darf nicht mehr als 10 betragen. Sie können Ihrem Zertifikat also bis zu 9 alternative Domains und Subdomains hinzufügen. Sie sollten die Einträge analog zu denen in der folgenden Liste hinzufügen.

- example.com
- example.net
- blog.example.com
- myexamples.com

So erstellen Sie ein Zertifikat mit alternativen Domains und Subdomains

1. Erstellen Sie einen Load Balancer, falls Sie noch keinen haben.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie Ihren Lightsail-Load Balancer.
4. Wählen Sie die Registerkarte Custom domains (Benutzerdefinierte Domains).
5. Wählen Sie Create certificate (Zertifikat erstellen).
6. Geben Sie einen Namen für Ihr Zertifikat ein oder übernehmen Sie den Standardnamen.

   Ressourcennamen:

   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

7. Geben Sie Ihre primäre Domain (`www.example.com`) und bis zu 9 alternative Domains oder Subdomains ein.
8. Wählen Sie Create certificate (Zertifikat erstellen).

   Nach der Erstellung der Domain haben Sie für die Überprüfung, dass Sie deren Eigentümer sind, 72 Stunden Zeit.

Nächste Schritte

- Überprüfen des Domain-Eigentümers mithilfe des DNS

  Nach erfolgter Bestätigung können Sie das validierte Zertifikat auswählen, um es mit Ihrem Lightsail-Load Balancer zu verknüpfen.
- Aktivieren der Sitzungspersistenz

Überprüfen eines SSL-/TLS-Zertifikats in Amazon Lightsail

Nachdem Sie ein SSL/TLS-Zertifikat in Lightsail erstellt haben, müssen Sie überprüfen, ob Sie die Kontrolle über alle Domänen und Subdomänen haben, die Sie dem Zertifikat hinzugefügt haben.

Inhalt

Schritt 1: Erstellen einer Lightsail-DNS-Zone für Ihre Domäne

Erstellen Sie eine Lightsail-DNS-Zone für Ihre Domäne, sofern Sie diesen Vorgang noch nicht ausgeführt haben. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain

Schritt 2: Hinzufügen von Datensätzen zur DNS-Zone Ihrer Domäne

Das Zertifikat, das Sie erstellt haben, bietet eine Reihe von kanonischen Namensdatensätzen (CNAME). Fügen Sie diese Datensätze der DNS-Zone Ihrer Domäne hinzu, um zu verifizieren, ob Sie die Domäne besitzen oder kontrollieren.

> **Important**
>
> Lightsail versucht, automatisch zu überprüfen, ob Sie die Kontrolle über die Domänen oder Subdomänen haben, die Sie bei der Erstellung des Zertifikats angegeben haben. Nachdem Sie Create certificate (Zertifikat erstellen) ausgewählt haben, werden die CNAME-Datensätze der DNS-Zone Ihrer Domäne hinzugefügt. Der Status des Zertifikats ändert sich von Attempting to validate your certificate (Es wird versucht, Ihr Zertifikat zu validieren) in Valid, in use (Gültig, in Gebrauch), wenn die automatische Validierung erfolgreich ist. Fahren Sie mit den folgenden Schritten fort, falls die automatische Validierung fehlschlägt.

In den folgenden Schritten erfahren Sie, wie Sie die CNAME-Datensätze abrufen und sie zur DNS-Zone Ihrer Domäne in der Lightsail-Konsole hinzufügen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite im oberen Navigationsmenü Account (Konto) aus.
3. Wählen Sie im Dropdown-Menü Konto aus.
4. Wählen Sie die Registerkarte Certificates (Zertifikate) aus.
5. Suchen Sie das Zertifikat, das Sie überprüfen möchten und notieren Sie sich Name und Value (Wert) der CNAME-Datensätze, die Sie für jede aufgelistete Domäne hinzufügen müssen.

   Drücken Sie Strg+C, wenn Sie Windows verwenden, oder Cmd+C, wenn Sie Mac verwenden, um sie in die Zwischenablage zu kopieren.

6. Öffnen Sie einen Text-Editor, wie z. B. Notepad, wenn Sie Windows verwenden, oder TextEdit, wenn Sie mit Mac arbeiten. Drücken Sie in der Textdatei Strg+V, wenn Sie Windows verwenden, oder Cmd+V, wenn Sie mit Mac arbeiten, um die Werte in die Textdatei einzufügen.

   Lassen Sie diese Textdatei geöffnet. Sie benötigen diese CNAME-Werte beim Hinzufügen der Datensätze zur DNS-Zone Ihrer Domäne später in diesem Handbuch.

7. Wählen Sie Startseite in der oberen Navigationsleiste der Lightsail-Konsole aus.
8. Wählen Sie auf der Lightsail-Startseite Domains & DNS (Domänen und DNS) aus.
9. Wählen Sie die DNS-Zone für die Domäne aus, für die das Zertifikat verwendet wird.
10. Wählen Sie auf der Registerkarte DNS records (DBS-Datensätze) die Option Add record (Datensatz hinzufügen) aus.
11. Wählen Sie für den Datensatztyp CNAME aus.
12. Gehen Sie zur Textdatei mit den CNAME-Datensätzen für Ihre Zertifikate.

    Kopieren Sie den Wert Name des CNAME-Datensatzes. Zum Beispiel `_1bfb0b9ef15a50f9041e559d2c67b760`.
13. Wechseln Sie zur Seite mit den DNS-Datensätzen und fügen Sie den Namen in das Feld Record name (Datensatzname) ein.

> **Important**
>
> Das Hinzufügen eines CNAME-Datensatzes, der einen Domänennamen (wie `.example.com`) enthält, kann zur Duplizierung des Domänennamens (wie

`.example.com.example.com`) führen. Um die Duplizierung zu vermeiden, bearbeiten Sie den Eintrag so, dass nur der Teil des CNAME, den Sie benötigen, hinzugefügt wird. Dies wäre `_1bfb0b9ef15a50f9041e559d2c67b760`.

14. Kopieren Sie den Wert des CNAME-Datensatzes. Zum Beispiel `_c9a0c385eda13283350e35f297469a13.hkvuiqjoua.acm-validations.aws..`
15. Wechseln Sie zur Seite mit den DNS-Datensätzen und fügen Sie den Wert in das Feld Route traffic to (Datenverkehr weiterleiten an) ein.
16. Klicken Sie auf Save (Speichern), um den Datensatz zu speichern.
17. Wenn Sie über alternative Unterdomänen verfügen, wählen Sie Datensatz hinzufügen aus, um einen weiteren Datensatz hinzuzufügen.

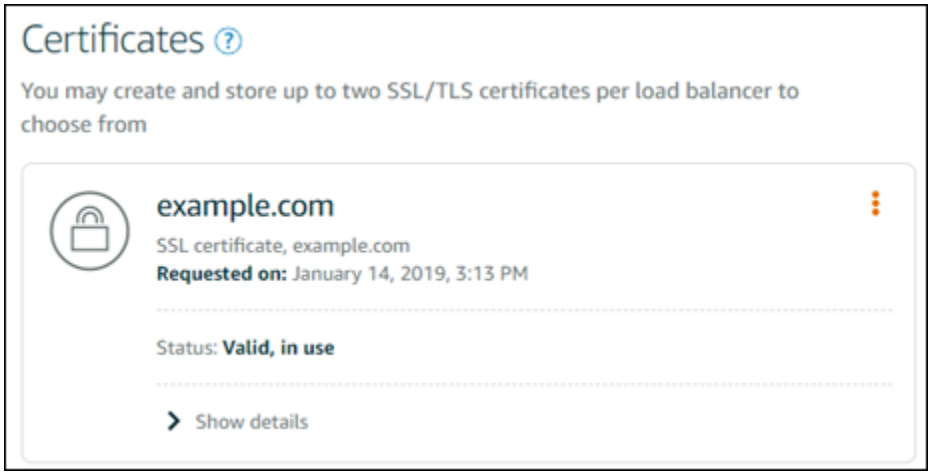
    > **Note**
    >
    > Weitere Informationen zu alternativen Domänen oder Unterdomänen finden Sie unter Hinzufügen von alternativen Domänen und Unterdomänen zu Ihrem SSL-/TLS-Zertifikat in Amazon Lightsail.

18. Wiederholen Sie die Schritte 11 bis 17 zum Hinzufügen der CNAME-Datensätze für die alternativen Unterdomänen.

    Auf der Verwaltungsseite der DNS-Zonen können Sie auch einen Aliasdatensatz (A) hinzufügen, um auf Ihren Load Balancer zu verweisen, oder andere Lightsail-Ressourcen.

    Wenn Sie fertig sind, sollte Ihre DNS-Zone wie im folgenden Screenshot aussehen.

Nach einiger Zeit wird Ihre Domäne verifiziert und die folgende Meldung auf dem Zertifikat angezeigt.

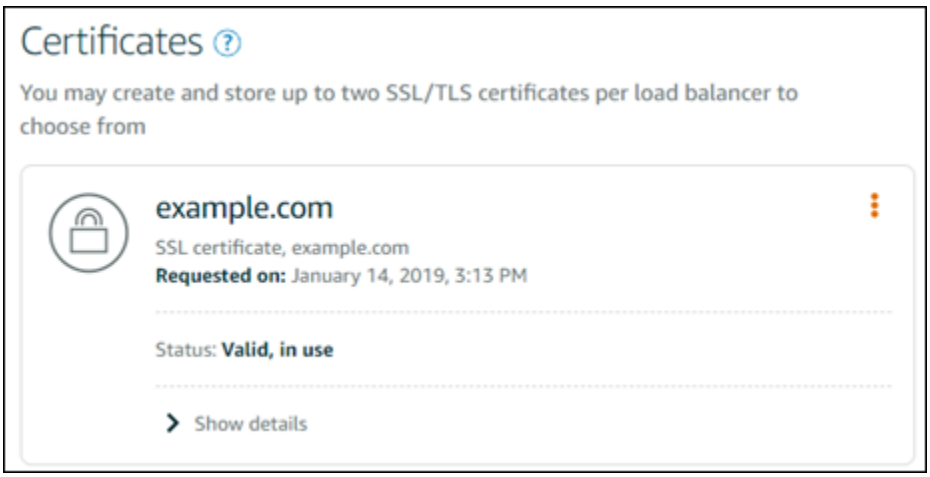


Nächster Schritt

Sobald Ihre Domain verifiziert wurde, können Sie ein gültiges SSL-/TLS-Zertifikat an Ihren Load Balancer anfügen.

Anfügen eines gültigen SSL-/TLS-Zertifikats an den Amazon Lightsail-Load Balancer

Nachdem Sie überprüft haben, dass Sie die Kontrolle über Ihre Domain haben, ändert sich der Status des Zertifikats in Valid (Gültig).



Im nächsten Schritt fügen Sie dem Lightsail-Load Balancer das Zertifikat an.

1. Klicken Sie auf der Lightsail-Startseite auf Networking (Netzwerk).
2. Wählen Sie Ihren -Load Balancer.
3. Wählen Sie die Registerkarte Custom domains (Benutzerdefinierte Domains).
4. Wählen Sie im Abschnitt Certificates (Zertifikate) die Option Attach certificate (Zertifikat anfügen) aus.
5. Wählen Sie ein Zertifikat aus der Dropdown-Liste aus.
6. Wählen Sie Attach (Anfügen), um das Zertifikat anzufügen.

Löschen eines SSL/TLS-Zertifikats in Amazon Lightsail

Sie können ein SSL/TLS-Zertifikat löschen, das Sie nicht mehr verwenden. Beispielsweise könnte Ihr Zertifikat abgelaufen sein und Sie haben bereits ein aktualisiertes und validiertes Zertifikat

zugewiesen. Wenn Sie Ihr Zertifikat vor dem Löschen duplizieren möchten, können Sie im gleichen Kontextmenü auch Duplicate (Duplizieren) auswählen, wie in Schritt 5 unten gezeigt.

> **Important**
>
> Wenn das zu löschende Zertifikat gültig und in Gebrauch ist, kann Ihr Load Balancer den verschlüsselten (HTTPS) Datenverkehr nicht mehr verarbeiten. Ihr Lightsail-Load-Balancer unterstützt weiterhin unverschlüsselten (HTTP) Datenverkehr.
> Löschen eines SSL-/TLS-Zertifikats ist endgültig und kann nicht rückgängig gemacht werden. Sie haben ein Kontingent für die Zertifikate, die Sie über einen Zeitraum von 365 Tagen erstellen können. Weitere Informationen finden Sie unter Kontingente im AWS Certificate Manager-Benutzerhandbuch.

1. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Networking (Netzwerk).
2. Wählen Sie den Load Balancer aus, an den das SSL/TLS-Zertifikat angefügt ist.
3. Wählen Sie die Registerkarte Eingehender Datenverkehr auf der Seite Ihrer Lastenverteilungsverwaltung.
4. Im Abschnitt Zertifikate auf der Seite, wählen Sie das Ellipsen-Symbol (⋮) für das Zertifikat, das Sie löschen möchten,und wählen Sie Löschen.

   DieLöschenist nicht verfügbar, wenn das Zertifikat, das Sie löschen möchten, verwendet wird. Um verwendete Zertifikate zu löschen, müssen Sie zuerst das Zertifikat des Lastausgleichsdienstes ändern, der das Zertifikat verwendet, oder HTTPS auf dem Lastausgleichsdienst deaktivieren, der das Zertifikat verwendet.

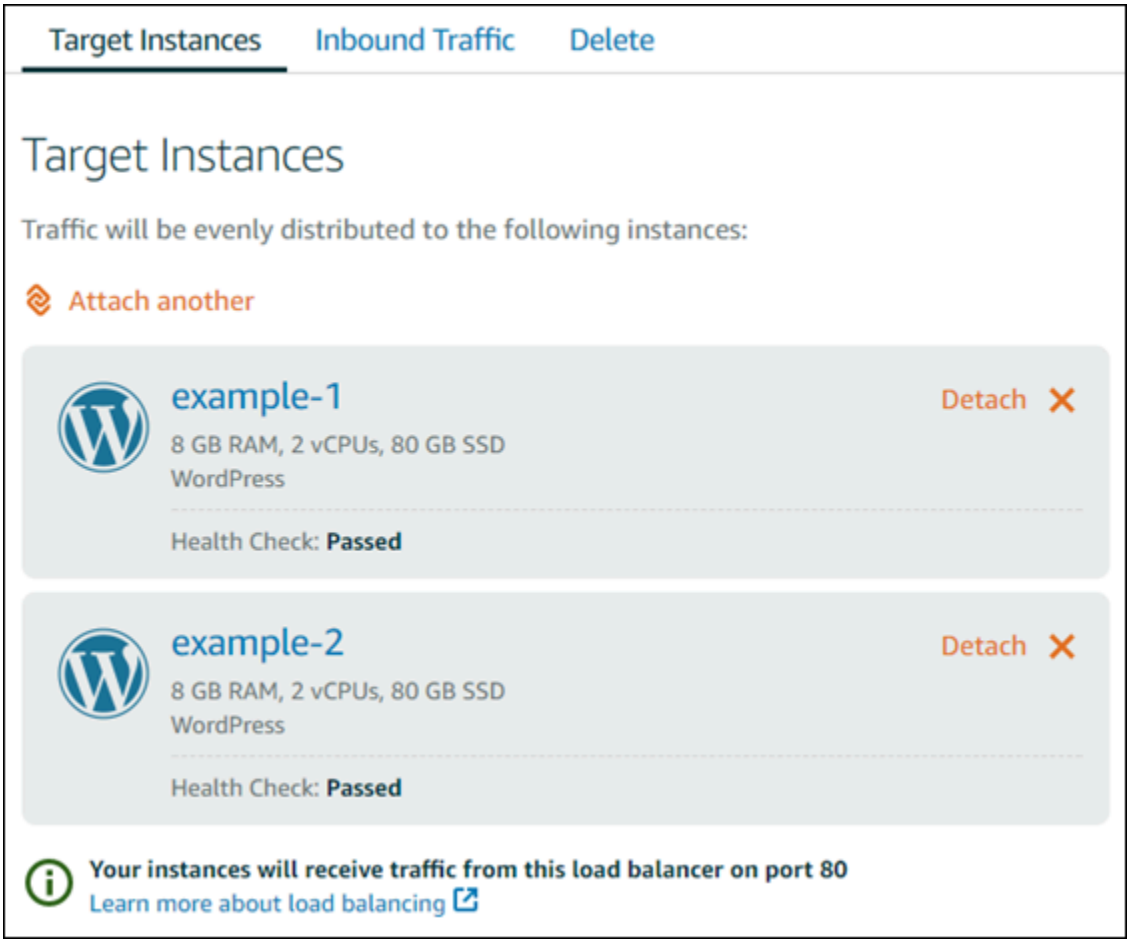
Aktualisieren der Amazon Lightsail-Load Balancer-Einstellungen

Wenn Sie einen Lightsail-Load Balancer erstellen, geben Sie nur die AWS-Region und den Namen an. In diesem Thema erfahren Sie, wie Sie den Load Balancer aktualisieren, um weitere Optionen zu aktivieren.

Falls noch nicht geschehen, müssen Sie einen Load Balancer erstellen. Erstellen eines Load Balancers

Health checks (Zustandsprüfungen)

Als Erstes sollten Sie Eine Instance für den Load Balancer konfigurieren. Danach können Sie dem Load Balancer eine Instance anfügen. Das Anfügen einer Instance startet den Zustandsprüfungsprozess und Sie erhalten auf der Verwaltungsseite des Load Balancers eine Passed (Erfolgreich)- oder Failed (Fehlgeschlagen)-Benachrichtigung.



Sie können auch den Pfad für die Zustandsprüfung anpassen. Wenn beispielsweise die Startseite langsam lädt oder zahlreiche Bilder enthält, können Sie Lightsail konfigurieren, um eine andere, schneller geladene Seite zu überprüfen. Passen Sie Load Balancer-Zustandsprüfungspfade an

Verschlüsselter Datenverkehr (HTTPS)

Sie können HTTPS einrichten, um die Sicherheit für die Benutzer Ihrer Website zu erhöhen. Wenn Sie den Load Balancer einrichten, sind drei Schritte erforderlich, um ein SSL-/TLS-Zertifikat zu erstellen und zu validieren.

Weitere Informationen zu HTTPS

Sitzungspersistenz

Die Sitzungspersistenz ist nützlich, wenn Sie Sitzungsinformationen lokal im Browser des Benutzers speichern. Nehmen Sie zum Beispiel an, dass Sie eine Magento-E-Commerce-Anwendung mit einem Einkaufswagen auf Lightsail ausführen. Bei aktivierter Sitzungspersistenz können die Benutzer dem Einkaufswagen Artikel hinzufügen und ihre Sitzung beenden. Wenn die Benutzer zurückkehren, befinden sich die Artikel immer noch im Einkaufswagen.

Sie können auch die Cookie-Dauer für die persistente Sitzung anpassen. Dies ist nützlich, wenn Sie eine besonders lange oder kurze Dauer haben möchten. Weitere Informationen finden Sie unter Aktivieren der Sitzungspersistenz für einen Load Balancer.

Konfigurieren einer Lightsail-Instance für Load Balancing

Bevor Sie Instances zu Ihrem Lightsail-Load-Balancer zuweisen, müssen Sie die Konfiguration Ihrer Anwendung evaluieren. Zum Beispiel funktionieren Load-Balancer oft besser, wenn die Datenschicht vom Rest der Anwendung getrennt ist. In diesem Thema erfahren Sie mehr über jede einzelne Lightsail-Instance und erhalten Empfehlungen dazu, ob Sie ein Load-Balancing ausführen sollten (oder horizontal skalieren) und wie Sie Ihre Anwendung am besten konfigurieren.

Allgemeine Richtlinien: Anwendungen mit Datenbank

Für Lightsail-Anwendungen, die eine Datenbank verwenden, empfehlen wir Ihnen, die Datenbank-Instance vom Rest Ihrer Anwendung zu trennen, damit Sie nur eine Datenbank-Instance haben. Der Hauptgrund ist, dass Sie vermeiden sollten, Daten in mehrere Datenbanken zu schreiben. Wenn Sie keine einzelne Datenbank-Instance anlegen, werden die Daten in die Datenbank der Instance geschrieben, die der Benutzer nutzt.

WordPress

Horizontale Skalierung? Ja, für einen WordPress-Blog oder -Website.

Konfigurationsempfehlungen vor dem Einsatz eines Lightsail-Load-Balancers

- Trennen Sie Ihre Datenbank so, dass jede WordPress-Instance, die hinter dem Load Balancer läuft, Informationen über dieselbe Stelle speichert und abruft. Wenn Sie mehr Leistung aus Ihrer Datenbank benötigen, können Sie die Rechenleistung oder den Speicher unabhängig von Ihrem Webserver replizieren oder ändern.

- Laden Sie Ihre Dateien und statischen Inhalte in einen Lightsail-Bucket ab. Um dies zu tun, müssen Sie das WP Offload Media Lite-Plug-In auf Ihrer WordPress-Website installieren und es so konfigurieren, dass eine Verbindung zu Ihrem Lightsail-Bucket herstellt. Weitere Informationen finden Sie im Tutorial: Verbinden einer WordPress-Instance zu einem Speicher-Bucket.

Node.js

Horizontale Skalierung? Ja, mit einigen Voraussetzungen.

Konfigurationsempfehlungen vor dem Einsatz eines Lightsail-Load-Balancers

- In Lightsail enthält der Node.js-Stack, verpackt von Bitnami, die Komponenten Node.js, Apache, Redis (eine In-Memory-Datenbank) und Python. Abhängig von der bereitgestellten Anwendung können Sie das Load-Balancing auf einigen wenigen Servern durchführen. Sie müssen jedoch einen Load-Balancer konfigurieren, um den Datenverkehr zwischen allen Webservern auszugleichen und Redis auf einen anderen Server zu verlagern.
- Verschieben Sie den Redis-Server auf einen anderen Server, um mit allen Instances zu kommunizieren. Fügen Sie ggf. einen Datenbankserver hinzu.
- Einer der Hauptanwendungsfälle für Redis ist die lokale Zwischenspeicherung von Daten, sodass Sie nicht ständig auf die zentrale Datenbank zugreifen müssen. Wir empfehlen Ihnen, die Session-Persistenz zu aktivieren, um die Performance-Verbesserung von Redis zu nutzen. Weitere Informationen finden Sie unter Aktivieren der Sitzungspersistenz für einen Load Balancer.
- Sie können außerdem einen gemeinsam genutzten Redis-Knoten verwenden. So können Sie Knoten gemeinsam nutzen oder einen lokalen Cache mit Sitzungspersistenz auf den einzelnen Maschinen verwenden.
- Wenn Sie einen Load Balancer mit Apache bereitstellen wollen, sollten Sie die Einbindung des `mod_proxy_balancer` in den Apache-Server in Betracht ziehen.

Weitere Informationen finden Sie unter Skalieren von Node.js-Anwendungen.

Magento

Horizontale Skalierung? Ja.

Konfigurationsempfehlungen vor dem Einsatz eines Lightsail-Load-Balancers

- Sie können eine AWS-Referenzbereitstellung von Magento verwenden. Diese verwendet zusätzliche Komponenten, z. B. eine Amazon-RDS-Datenbank: Terraform Magento Adobe Commerce in AWS.
- Vergewissern Sie sich, dass die Sitzungspersistenz aktiviert ist. Magento verwendet einen Einkaufswagen. Dies hilft sicherzustellen, dass Kunden mit mehreren Besuchen über mehrere Sitzungen hinweg bei ihrer Rückkehr die Artikel in ihrem Einkaufswagen vorfinden. Weitere Informationen finden Sie unter Aktivieren der Sitzungspersistenz für einen Load Balancer.

GitLab

Horizontale Skalierung? Ja, mit Voraussetzungen.

Konfigurationsempfehlungen vor dem Einsatz eines Lightsail-Load-Balancers

Sie benötigen Folgendes:

- Ein ausgeführter und betriebsbereiter Redis-Knoten.
- Ein gemeinsam genutzter Network Storage Server (NFS)
- Eine zentrale Datenbank (MySQL oder PostgreSQL) für die Anwendung. Siehe die allgemeinen Richtlinien zu Datenbanken oben.

Weitere Informationen finden Sie unter High Availability (Hochverfügbarkeit) auf der GitLab-Website.

> **Note**
>
> Der in oben erwähnte gemeinsame Network Storage Server (NFS) ist derzeit mit der GitLab-Vorlage nicht verfügbar.

Drupal

Horizontale Skalierung? Ja. Drupal bietet ein offizielles Dokument, das beschreibt, wie Sie Ihre Anwendung horizontal skalieren können: Server Scaling.

Konfigurationsempfehlungen vor dem Einsatz eines Lightsail-Load-Balancers

Sie müssen ein Drupal-Modul einrichten, um Dateien zwischen verschiedenen Instances zu synchronisieren. Die Drupal-Website verfügt über mehrere Module. Sie sind jedoch mehr für das Prototyping als für den Produktionseinsatz geeignet.

Verwenden Sie ein Modul, mit dem Sie Ihre Dateien in Amazon S3 speichern können. Dadurch erhalten Sie einen zentralen Ort für Ihre Dateien, anstatt separate Kopien auf jeder Ziel-Instance zu speichern. Wenn Sie Ihre Dateien bearbeiten, werden die Aktualisierungen so aus dem zentralen Speicher übernommen und Ihre Benutzer sehen dieselben Dateien, unabhängig davon, auf welche Instance sie treffen.

- Amazon-S3-Dateisystem
- Inhaltssynchronisation

Weitere Informationen finden Sie unter Horizontales Skalieren von Drupal und in der Cloud.

LAMP-Stack

Horizontale Skalierung? Ja.

Konfigurationsempfehlungen vor dem Einsatz eines Lightsail-Load-Balancers

- Sie sollten eine Datenbank in einer separaten Instance anlegen. Alle Instances hinter dem Load Balancer sollten auf diese separate Datenbank-Instance zeigen, damit sie Informationen an derselben Stelle speichern und abrufen können.
- Abhängig von der bereitzustellenden Anwendung sollten Sie das gemeinsam genutzte Dateisystem festlegen (NFS, Lightsail-Blockspeicherdatenträger oder Amazon-S3-Speicher).

MEAN-Stack

Horizontale Skalierung? Ja.

Konfigurationsempfehlungen vor dem Einsatz eines Lightsail-Load-Balancers

Verschieben Sie MongoDB auf einen anderen Rechner und konfigurieren Sie einen Mechanismus, um das Root-Dokument für die Lightsail-Instances freizugeben.

Redmine

Horizontale Skalierung? Ja.

Konfigurationsempfehlungen vor dem Einsatz eines Lightsail-Load-Balancers

- Nutzen Sie das Redmine_S3-Plugin, um die Anhänge in Amazon S3 statt im lokalen Dateisystem zu speichern.
- Trennen Sie die Datenbank in einer anderen Instance.

Nginx

Horizontale Skalierung? Ja.

Sie können eine oder mehrere Lightsail-Instances mit Nginx nutzen, die an einem Lightsail-Load-Balancer angefügt sind. Weitere Informationen finden Sie unter Scaling Web Applications with NGINX, Part 1: Load Balancing.

Joomla!

Horizontale Skalierung? Ja, mit Voraussetzungen.

Konfigurationsempfehlungen vor dem Einsatz eines Lightsail-Load-Balancers

Obwohl es keine offizielle Dokumentation auf der Joomla-Website gibt, gibt es einige Diskussionen in ihren Community-Foren. Einige Benutzer haben es geschafft, ihre Joomla-Instances horizontal zu skalieren, indem sie einen Cluster mit der folgenden Konfiguration nutzen:

- Ein Lightsail-Load-Balancer, der so konfiguriert ist, dass er eine Sitzungspersistenz ermöglicht. Weitere Informationen finden Sie unter Aktivieren der Sitzungspersistenz für einen Load Balancer.
- Mehrere Lightsail-Instances mit Joomla, die an den Load Balancer angefügt sind, werden mit dem Dokumentenstamm von Joomla! synchronisiert. Sie können dazu Tools wie Rsync verwenden, einen NFS-Server haben, der für die Synchronisierung der Inhalte zwischen allen Lightsail-Instances zuständig ist, oder über den Dateien per AWS teilen.
- Mehrere Datenbankserver, die mit einem Replikationscluster konfiguriert sind.
- In jeder Lightsail-Instance ist das gleiche Cachesystem konfiguriert. Es gibt einige nützliche Erweiterungen, wie z. B. JotCache.

Konfigurieren Sie TLS-Sicherheitsrichtlinien auf Ihrem Amazon Lightsail Load Balancer

Nachdem Sie HTTPS auf Ihrem Amazon Lightsail Load Balancer aktiviert haben, können Sie eine TLS-Sicherheitsrichtlinie für die verschlüsselten Verbindungen konfigurieren. Dieses Handbuch enthält Informationen zu den Sicherheitsrichtlinien, die Sie auf Lightsail-Load Balancern konfigurieren können, sowie zu den Verfahren zur Aktualisierung der Sicherheitsrichtlinien Ihres Load Balancers. Weitere Informationen über Load Balancer finden Sie unter Load Balancer.

Übersicht über die Sicherheitsrichtlinien

Lightsail Load Balancing verwendet eine Secure Socket Layer (SSL) -Verhandlungskonfiguration, die als Sicherheitsrichtlinie bezeichnet wird, um SSL-Verbindungen zwischen einem Client und dem Load Balancer auszuhandeln. Eine Sicherheitsrichtlinie ist eine Kombination aus Protokollen und Verschlüsselungen. Das Protokoll stellt eine sichere Verbindung zwischen einem Client und einem Server her und stellt sicher, dass alle Daten, die zwischen dem Client und Ihres Load Balancers übertragen werden, privat sind. Ein Verschlüsselungsverfahren ist ein Algorithmus, der eine kodierte Nachricht mithilfe von Verschlüsselungsschlüsseln erstellt. Protokolle verwenden mehrere Verschlüsselungsverfahren zum Verschlüsseln von Daten über das Internet. Während der Verbindungsaushandlung präsentieren der Client und der Load Balancer eine Liste von Verschlüsselungsverfahren und Protokollen, die sie jeweils unterstützen, nach Priorität sortiert. Standardmäßig wird für die sichere Verbindung die erste Verschlüsselung auf der Liste des Servers ausgewählt, die mit einem der Verschlüsselungsverfahren des Clients übereinstimmt. Lightsail Load Balancer unterstützen keine SSL-Neuverhandlung für Client- oder Zielverbindungen.

Die `TLS-2016-08` Sicherheitsrichtlinie wird standardmäßig konfiguriert, wenn Sie HTTPS auf einem Lightsail-Load Balancer aktivieren. Sie können nach Bedarf eine andere Sicherheitsrichtlinie konfigurieren, wie weiter unten in diesem Leitfaden beschrieben. Sie können die Sicherheitsrichtlinie auswählen, die nur für Frontend-Verbindungen verwendet wird. Die `TLS-2016-08`-Sicherheitsrichtlinie wird immer für Backend-Verbindungen verwendet. Lightsail Load Balancer unterstützen keine benutzerdefinierten Sicherheitsrichtlinien.

Unterstützte Sicherheitsrichtlinien und -protokolle

Lightsail Load Balancer können mit den folgenden Sicherheitsrichtlinien und Protokollen konfiguriert werden:

Security policies	TLS-2016-08 (default)	TLS-FS-1-2-Res-2019-08
TLS Protocols		
Protocol-TLSv1	✓	
Protocol-TLSv1.1	✓	
Protocol-TLSv1.2	✓	✓
TLS Ciphers		
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓	✓
ECDHE-RSA-AES128-SHA256	✓	✓
ECDHE-ECDSA-AES128-SHA	✓	
ECDHE-RSA-AES128-SHA	✓	
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓	✓
ECDHE-RSA-AES256-SHA384	✓	✓
ECDHE-RSA-AES256-SHA	✓	
ECDHE-ECDSA-AES256-SHA	✓	
AES128-GCM-SHA256	✓	
AES128-SHA256	✓	
AES128-SHA	✓	

Sorgen Sie dafür, dass die Voraussetzungen erfüllt sind.

Erfüllen Sie die folgenden Voraussetzungen, wenn dies noch nicht geschehen ist:

- Erstellen eines Load Balancers und Anfügen von Instances. Weitere Informationen finden Sie unter Erstellen eines Load Balancers und Anfügen von Instances.
- Erstellen Sie ein SSL-/TLS-Zertifikat und hängen Sie es an Ihren Load Balancer an, um HTTPS zu aktivieren. Weitere Informationen finden Sie unter Erstellen eines SSL-/TLS-Zertifikats für Ihren Lightsail-Load-Balancer. Weitere Informationen zu Zertifikaten finden Sie unter SSL-/TLS-Zertifikate in.

Konfigurieren Sie eine Sicherheitsrichtlinie mit der Lightsail-Konsole

Gehen Sie wie folgt vor, um eine Sicherheitsrichtlinie mithilfe der Lightsail-Konsole zu konfigurieren.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Networking (Netzwerk).
3. Wählen Sie den Namen des Load Balancers, für die Sie eine TLS-Sicherheitsrichtlinie konfigurieren möchten.
4. Wählen Sie die Registerkarte Inbound traffic (Eingehender Datenverkehr) aus.
5. Klicken Sie auf Protokolle ändern unter dem Abschnitt TLS-Sicherheitsprotokolle der Seite.
6. Wählen Sie eine der folgenden Optionen im Dropdown-Menü Unterstützte Protokolle:

   - TLS Version 1.2 – Diese Option ist die sicherste, aber ältere Browser können eventuell keine Verbindung mehr herstellen.
   - TLS Version 1.0, 1.1 und 1.2 – Diese Option bietet die beste Kompatibilität mit Browsern.
7. Klicken Sie auf Save (Speichern), um das ausgewählte Protokoll auf Ihren Load Balancer anzuwenden.

   Es dauert einen Moment, bis Ihre Änderung wirksam wird.

Konfigurieren Sie eine Sicherheitsrichtlinie mit dem AWS CLI

Führen Sie das folgende Verfahren durch, um eine Sicherheitsrichtlinie mithilfe der AWS Command Line Interface (AWS CLI) zu konfigurieren. Führen Sie dazu den Befehl `update-load-balancer-`

`attribute` aus. Weitere Informationen finden Sie update-load-balancer-attributein der AWS CLI Befehlsreferenz.

> **Note**
>
> Sie müssen Lightsail installieren AWS CLI und konfigurieren, bevor Sie mit diesem Verfahren fortfahren können. Weitere Informationen finden Sie unter So konfigurieren, AWS CLI dass es mit Lightsail funktioniert.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um die TLS-Sicherheitsrichtlinie für Ihren Load Balancer zu ändern.

```
aws lightsail update-load-balancer-attribute --load-balancer-name LoadBalancerName
 --attribute-name TlsPolicyName --attribute-value AttributeValue
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *LoadBalancerName*mit dem Namen des Load Balancers, für den Sie die TLS-Sicherheitsrichtlinie ändern möchten.
- *AttributeValue*mit der `TLS-FS-1-2-Res-2019-08` Sicherheitsrichtlinie `TLS-2016-08` oder.

> **Note**
>
> Das Attribut `TlsPolicyName` im Befehl gibt an, dass Sie die TLS-Sicherheitsrichtlinie bearbeiten möchten, die für den Load Balancer konfiguriert ist.

Beispiel:

```
aws lightsail update-load-balancer-attribute --load-balancer-name MyLoadBalancer --
attribute-name TlsPolicyName --attribute-value TLS-2016-08
```

Es dauert einen Moment, bis Ihre Änderung wirksam wird.

Konfigurieren der HTTP-zu-HTTPS-Umleitung für einen Lightsail-Load-Balancer

Nachdem Sie HTTPS auf Ihrem Amazon Lightsail-Load-Balancer konfiguriert haben, können Sie eine HTTP-zu-HTTPS-Umleitung konfigurieren, sodass Benutzer, die über eine HTTP-Verbindung auf Ihre Website oder Webanwendung zugreifen, automatisch auf die verschlüsselte HTTPS-Verbindung umgeleitet werden. Weitere Informationen über Load Balancer finden Sie unter Load Balancer.

Sorgen Sie dafür, dass die Voraussetzungen erfüllt sind.

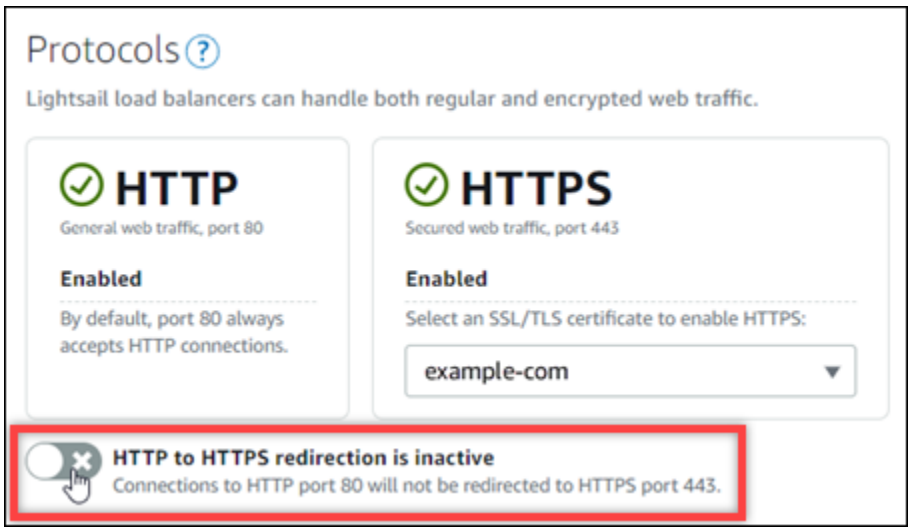
Erfüllen Sie die folgenden Voraussetzungen, wenn dies noch nicht geschehen ist:

- Erstellen eines -Load-Balancers und Anfügen von Instances. Weitere Informationen finden Sie unter Erstellen eines Load Balancers und Anfügen von Instances.
- Erstellen Sie ein SSL-/TLS-Zertifikat und hängen Sie es an Ihren Load Balancer an, um HTTPS zu aktivieren. Weitere Informationen finden Sie unter Erstellen eines SSL-/TLS-Zertifikats für Ihren Lightsail-Load-Balancer. Weitere Informationen zu Zertifikaten finden Sie unter SSL-/TLS-Zertifikate in.

Konfigurieren der HTTPS-Umleitung für Ihren Load Balancer mithilfe der Lightsail-Konsole

Führen Sie das folgende Verfahren aus, um die HTTPS-Umleitung für Ihren Load Balancer mithilfe der Lightsail-Konsole zu konfigurieren.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen des Load Balancers, für die Sie eine HTTPS-Umleitung konfigurieren möchten.
4. Wählen Sie die Registerkarte Inbound traffic (Eingehender Datenverkehr) aus.
5. Im Abschnitt Protokolle der Seite können Sie eine der folgenden Aktionen ausführen:



- Die Richtungsoption auf aktiv umschalten, um die HTTP-zu-HTTPS-Umleitung zu aktivieren.
- Die Richtungsoption auf inaktiv umschalten, um die HTTP-zu-HTTPS-Umleitung zu deaktivieren.

Es dauert einen Moment, bis Ihre Änderung wirksam wird.

Konfigurieren der HTTP-zu-HTTPS-Umleitung für einen Load Balancer mit AWS CLI

Führen Sie das folgende Verfahren aus, um die HTTPS-Umleitung für Ihren Load Balancer mithilfe der AWS Command Line Interface (AWS CLI) zu konfigurieren. Führen Sie dazu den Befehl `update-load-balancer-attribute` aus. Weitere Informationen finden Sie unter update-load-balancer-attribute in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail konfigurieren, bevor Sie mit diesem Vorgang fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um die HTTPS-Umleitung für Ihren Load Balancer zu konfigurieren.

```
aws lightsail update-load-balancer-attribute --load-balancer-name LoadBalancerName
 --attribute-name HttpsRedirectionEnabled --attribute-value AttributeValue
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *LoadBalancerName* mit dem Namen des Load Balancers, für die Sie die HTTP-zu-HTTPS-Umleitung aktivieren oder deaktivieren möchten.
- *AttributeValue* mit `true`, um die Umleitung zu aktivieren, oder `false`, um die Umleitung zu deaktivieren.

> **Note**
>
> Das Attribut `HttpsRedirectionEnabled` im Befehl gibt an, dass Sie bearbeiten möchten, ob die HTTPS-Umleitung für den angegebenen Load Balancer aktiviert oder deaktiviert wird.

Beispiele:

- So aktivieren Sie die HTTP-zu-HTTPS-Umleitung für Ihren Load Balancer:

```
aws lightsail update-load-balancer-attribute --load-balancer-name MyLoadBalancer
 --attribute-name HttpsRedirectionEnabled --attribute-value true
```

- So deaktivieren Sie die HTTP-zu-HTTPS-Umleitung für Ihren Load Balancer:

```
aws lightsail update-load-balancer-attribute --load-balancer-name MyLoadBalancer
 --attribute-name HttpsRedirectionEnabled --attribute-value false
```

Es dauert einen Moment, bis Ihre Änderung wirksam wird.

Aktivieren der Sitzungspersistenz für Lightsail-Load-Balancer

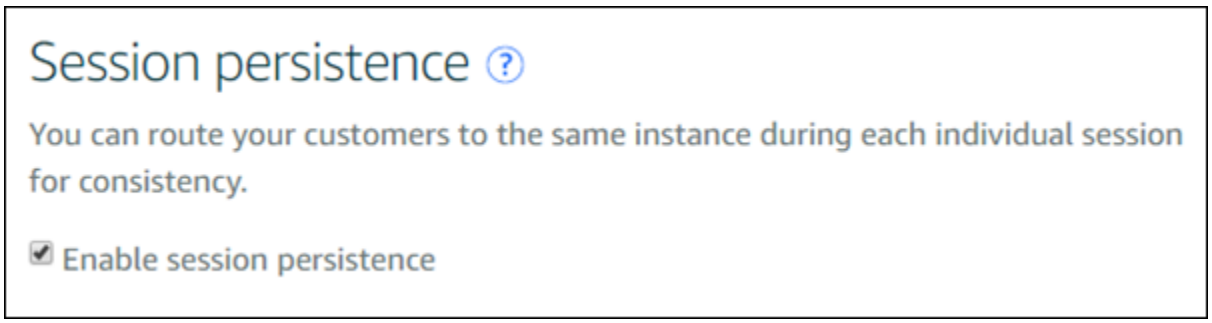
Sie können die Sitzungspersistenz für Ihre Benutzer aktivieren. Dies ist hilfreich, wenn Sie Sitzungsinformationen lokal im Browser des Benutzers speichern. Nehmen Sie zum Beispiel an, dass Sie eine Magento-E-Commerce-Anwendung mit einem Einkaufswagen auf Lightsail ausführen. Wenn

Sie die Sitzungspersistenz aktivieren, können Ihre Benutzer dem Einkaufswagen Artikel hinzufügen, die Website verlassen und finden bei Ihrer Rückkehr die Artikel immer noch im Einkaufswagen wieder.

Sie können die Cookie-Dauer auch mithilfe der AWS Command Line Interface (AWS CLI)- oder Lightsail-API anpassen.

Aktivieren der Sitzungspersistenz

1. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Networking (Netzwerk).
2. Markieren Sie Ihren Load Balancer, um ihn zu verwalten.
3. Wählen Sie die Registerkarte Inbound traffic (Eingehender Datenverkehr) aus.
4. Klicken Sie auf Enable session persistence (Sitzungspersistenz aktivieren).



Anpassen der Cookie-Dauer

Sie können auch die Cookie-Dauer für die persistente Sitzung anpassen. Dies ist nützlich, wenn Sie eine besonders lange oder kurze Dauer haben möchten. Für viele E-Commerce-Websites ist die Dauer beispielsweise sehr lang. Dadurch können Kunden die Website verlassen und finden ihre Artikel beim Zurückkehren in ihrem Einkaufswagen wieder.

Wenn Sie es noch nicht getan haben, müssen Sie AWS CLI einrichten und konfigurieren.

Konfigurieren der AWS Command Line Interface für die Arbeit mit Amazon Lightsail

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminal-Fenster.
2. Geben Sie den folgenden AWS CLI-Befehl ein, um die Cookie-Dauer auf drei Tage (259.200 Sekunden) auszuweiten.

```
aws lightsail update-load-balancer-attribute --load-balancer-name LoadBalancerName
 --attribute-name SessionStickiness_LB_CookieDurationSeconds --attribute-value
 259200
```

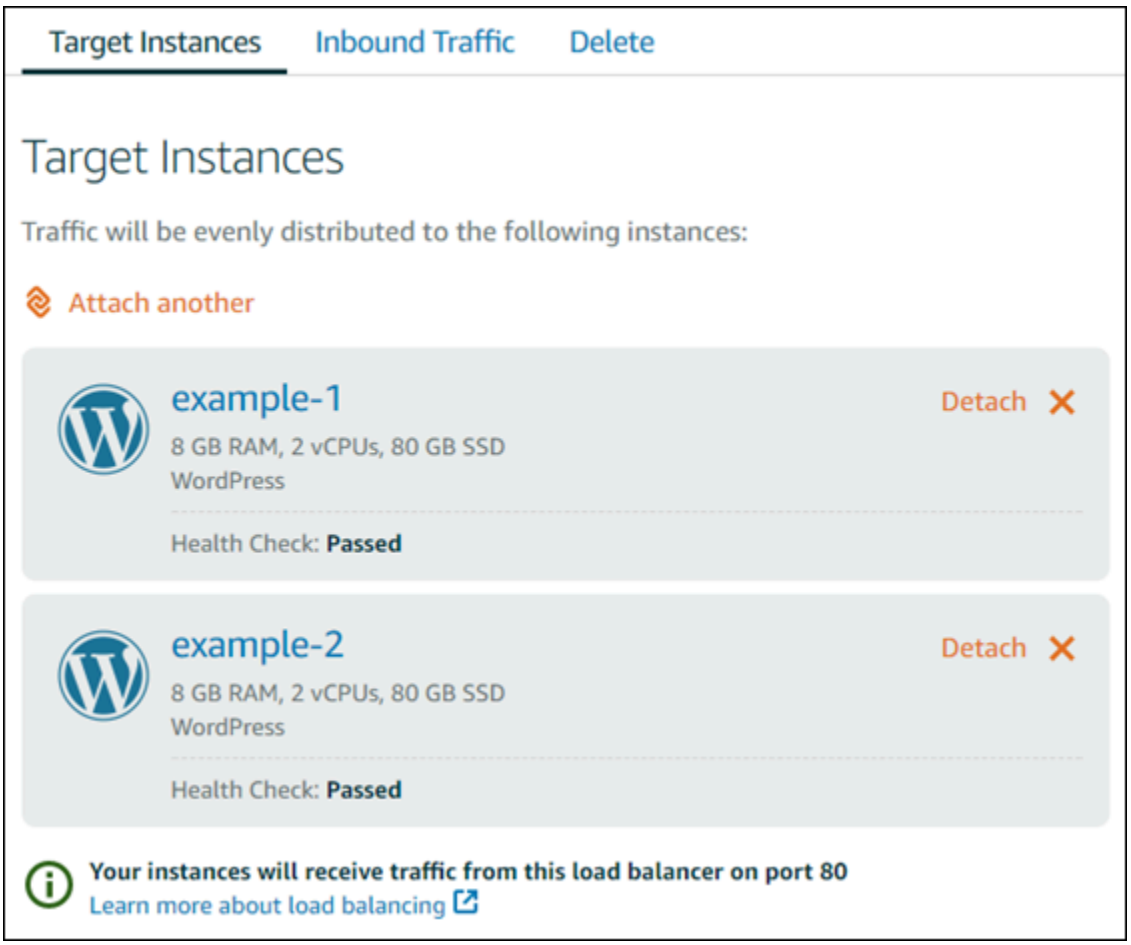
Ersetzen Sie im Befehl *LoadBalancerName* durch den Namen Ihres Load Balancers.

Bei Erfolg sollte die folgende Antwort angezeigt werden.

```
{
    "operations": [
        {
            "status": "Succeeded",
            "resourceType": "LoadBalancer",
            "isTerminal": true,
            "operationDetails": "SessionStickiness_LB_CookieDurationSeconds",
            "statusChangedAt": 1511758936.174,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "operationType": "UpdateLoadBalancerAttribute",
            "resourceName": "example-load-balancer",
            "id": "681c2bd9-9a51-402b-8ad2-12345EXAMPLE",
            "createdAt": 1511758936.174
        }
    ]
}
```

Zustandsprüfung für Amazon Lightsail-Load Balancer

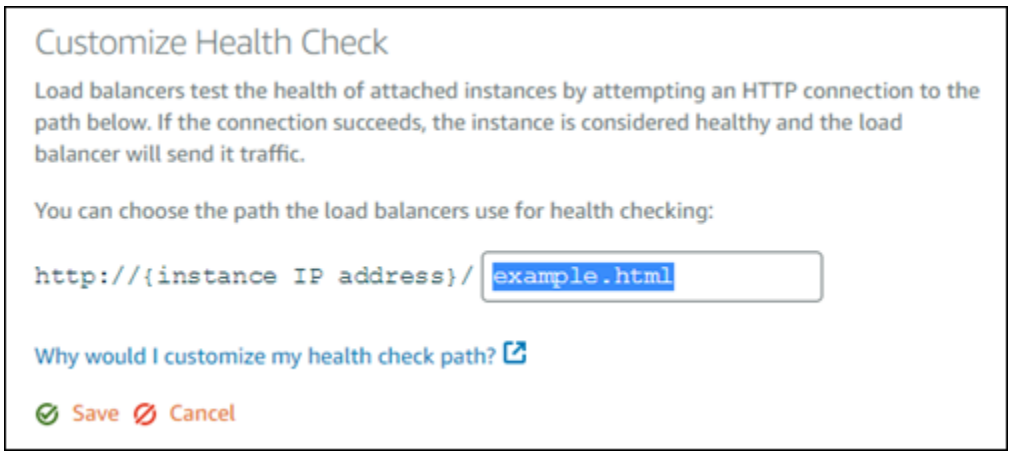
Die Zustandsprüfung beginnt, sobald Sie Ihre Lightsail-Instances an Ihren Load Balancer angefügt haben. Danach erfolgt sie alle 30 Sekunden. Sie können den Status der Zustandsprüfung auf der Verwaltungsseite vom Load Balancer ansehen.



Anpassen des Pfads für die Zustandsprüfung

Sie können den Pfad für die Zustandsprüfung anpassen. Wenn beispielsweise die Startseite langsam lädt oder zahlreiche Bilder enthält, können Sie Lightsail konfigurieren, um eine andere, schneller geladene Seite zu überprüfen.

1. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Networking (Netzwerk).
2. Markieren Sie Ihren Load Balancer, um ihn zu verwalten.
3. Wählen Sie auf der Registerkarte Target instances (Ziel-Instances) die Option Customize health checking (Zustandsprüfung anpassen) aus.
4. Geben Sie einen gültigen Pfad für die Zustandsprüfung ein und klicken Sie auf Save (Speichern).



Zustandsprüfungsmetriken

Mit den folgenden Metriken können Sie Probleme bei der Zustandsprüfung diagnostizieren. Verwenden Sie die AWS Command Line Interface oder die Lightsail-API, um Informationen über eine bestimmte Zustandsprüfungsmetrik zurückzugeben.

- **`ClientTLSNegotiationErrorCount`** - Die Anzahl der TLS-Verbindungen, die vom Client initiiert wurden und keine Sitzung mit dem Load Balancer hergestellt haben. Als mögliche Ursachen kommen unter anderem fehlende Übereinstimmung bei Verschlüsselungsverfahren oder Protokollen infrage.

  `Statistics`: Die nützlichste Statistik ist `Sum`.
- **`HealthyHostCount`** – Die Anzahl der Ziel-Instances, die als stabil betrachtet werden.

  `Statistics`: Die nützlichsten Statistiken sind `Average`, `Minimum` und `Maximum`.
- **`UnhealthyHostCount`** – Die Anzahl der Ziel-Instances, die als fehlerhaft betrachtet werden.

  `Statistics`: Die nützlichsten Statistiken sind `Average`, `Minimum` und `Maximum`.
- **`HTTPCode_LB_4XX_Count`** - Anzahl der HTTP-4XX-Client-Fehlercodes, die vom Load Balancer verursacht werden. Client-Fehler werden bei Anforderungen mit falschem Format oder unvollständigen Anforderungen generiert. Diese Anforderungen sind nicht von der Ziel-Instance empfangen worden. Diese Anzahl umfasst keine Antwortcodes, die von den Ziel-Instances generiert wurden.

  `Statistics`: Die nützlichste Statistik ist `Sum`. Beachten Sie, dass sowohl `Minimum` und `Maximum` als auch `Average` `1` zurückgeben.

- **`HTTPCode_LB_5XX_Count`** - Anzahl der HTTP-5XX-Server-Fehlercodes, die vom Load Balancer verursacht werden. Diese Anzahl umfasst keine Antwortcodes, die von den Ziel-Instances generiert wurden.

  `Statistics`: Die nützlichste Statistik ist `Sum`. Beachten Sie, dass sowohl `Minimum` und `Maximum` als auch `Average` 1 zurückgeben. Beachten Sie, dass sowohl `Minimum` und `Maximum` als auch `Average` 1 zurückgeben.

- **`HTTPCode_Instance_2XX_Count`** – Die Anzahl der HTTP-Antwortcodes, die von den Ziel-Instances generiert wurden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.

  `Statistics`: Die nützlichste Statistik ist `Sum`. Beachten Sie, dass sowohl `Minimum` und `Maximum` als auch `Average` 1 zurückgeben.

- **`HTTPCode_Instance_3XX_Count`** – Die Anzahl der HTTP-Antwortcodes, die von den Ziel-Instances generiert wurden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.

  `Statistics`: Die nützlichste Statistik ist `Sum`. Beachten Sie, dass sowohl `Minimum` und `Maximum` als auch `Average` 1 zurückgeben.

- **`HTTPCode_Instance_4XX_Count`** – Die Anzahl der HTTP-Antwortcodes, die von den Ziel-Instances generiert wurden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.

  `Statistics`: Die nützlichste Statistik ist `Sum`. Beachten Sie, dass sowohl `Minimum` und `Maximum` als auch `Average` 1 zurückgeben.

- **`HTTPCode_Instance_5XX_Count`** – Die Anzahl der HTTP-Antwortcodes, die von den Ziel-Instances generiert wurden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.

  `Statistics`: Die nützlichste Statistik ist `Sum`. Beachten Sie, dass sowohl `Minimum` und `Maximum` als auch `Average` 1 zurückgeben.

- **`InstanceResponseTime`** - Die verstrichene Zeit in Sekunden bis zum Empfang einer Antwort von der Ziel-Instance, nachdem die Anforderung den Load Balancer verlassen hat.

  `Statistics`: Die nützlichste Statistik ist `Average`.

- **`RejectedConnectionCount`** - Anzahl der abgelehnten Verbindungen, weil der Load Balancer die maximale Anzahl an Verbindungen erreicht hat.

`Statistics`: Die nützlichste Statistik ist `Sum`.

- **`RequestCount`** – Die Anzahl von Anforderungen, die per IPv4 verarbeitet wurden. In dieser Zahl sind nur die Anforderungen mit einer Antwort enthalten, die von einer Ziel-Instance des Load Balancers generiert wurden.

  `Statistics`: Die nützlichste Statistik ist `Sum`. Beachten Sie, dass sowohl `Minimum` und `Maximum` als auch `Average` `1` zurückgeben.

Themen

Status der Lightsail-Load-Balancer-Zustandsprüfung

Standardmäßig führt Lightsail Zustandsprüfungen Ihrer Instances an der Wurzel (`"/"`) Ihrer Webanwendung durch. Die Zustandsprüfungen dienen zur Überwachung der registrierten Instances, sodass der Load Balancer nur Anfragen an die fehlerfreien Instances senden kann. Die Zustandsprüfungen beginnen, sobald Sie dem Load Balancer die Instances angefügt haben.

Einer der folgenden Status wird zurückgegeben.

- Passed
- Fehlgeschlagen

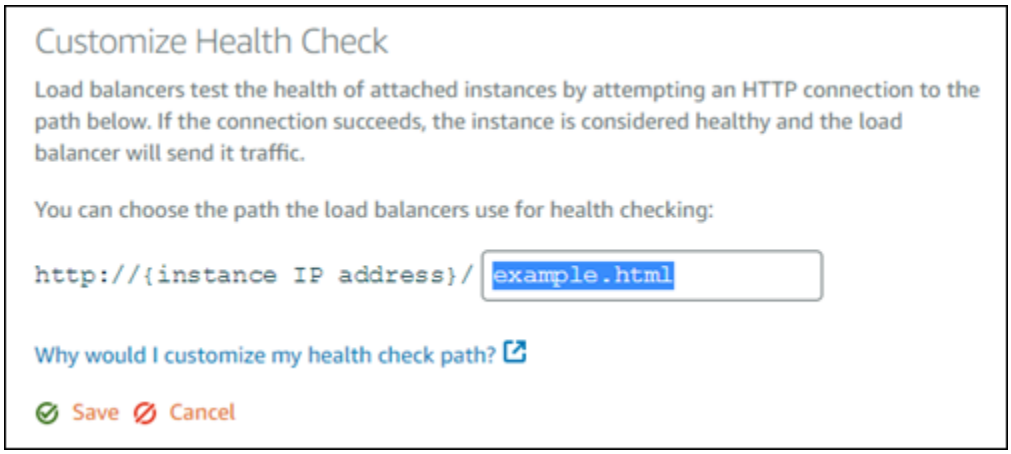
Wenn Ihre Zustandsprüfung fehlschlägt, können Sie den Fehler mit der AWS Command Line Interface oder der Lightsail-API analysieren. Weitere Informationen zur Fehlerbehebung finden Sie im Fehlerbehebungshandbuch.

Anpassen des Pfads für die Zustandsprüfung

Sie können den Pfad für die Zustandsprüfung anpassen. Wenn beispielsweise die Startseite langsam lädt oder zahlreiche Bilder enthält, können Sie Lightsail konfigurieren, um eine andere, schneller geladene Seite zu überprüfen.

1. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Networking (Netzwerk).
2. Markieren Sie Ihren Load Balancer, um ihn zu verwalten.

3. Wählen Sie auf der Registerkarte Target instances (Ziel-Instances) die Option Customize health checking (Zustandsprüfung anpassen) aus.
4. Geben Sie einen gültigen Pfad für die Zustandsprüfung ein und klicken Sie auf Save (Speichern).



Trennen von Instances von einem Lightsail-Load-Balancer

Wenn eine Instance nicht mehr an den Lightsail-Load-Balancer angefügt sein soll, können Sie sie trennen. Warten Sie, bis die angegebenen Instances nicht länger benötigt werden, bevor Sie eine Lightsail-Instance von einem Load Balancer trennen.

1. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Networking (Netzwerk).
2. Wählen Sie den Load Balancer aus, den Sie verwalten möchten.
3. Wählen Sie auf der Registerkarte Target instances (Ziel-Instances) neben dem Load Balancer, den Sie trennen möchten, die Option Detach (Trennen) aus.

Löschen eines Lightsail-Load-Balancers

Sie können einen Lightsail-Load-Balancer löschen, wenn Sie ihn nicht mehr benötigen Durch Löschen eines Load Balancers werden alle angefügten Lightsail-Instances zwar getrennt, die Lightsail-Instances werden aber nicht gelöscht. Wenn Sie verschlüsselten Datenverkehr (HTTPS) mit einem SSL-/TLS-Zertifikat aktiviert haben, werden durch Löschen des Load Balancers die zugehörigen SSL-/TLS-Zertifikate auch entfernt.

> **Important**
>
> Das Löschen eines Lightsail-Load-Balancers und die damit verbundenen Zertifikate ist endgültig und kann nicht mehr rückgängig gemacht werden.

1. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Networking (Netzwerk).
2. Wählen Sie den Load Balancer aus, den Sie löschen möchten.
3. Wählen Sie Delete (Löschen).
4. Klicken Sie auf Delete load balancer (Load Balancer löschen).
5. Wählen Sie Yes, delete (Ja, löschen) aus.

Netzwerkverteilungen für die Bereitstellung von Inhalten in Amazon Lightsail

Eine Lightsail-Verteilung verwendet ein global verteiltes Netzwerk von Servern, auch bekannt als Edge-Positionen, um Ihren Benutzern eine schnellere Bereitstellung Ihrer Inhalte zu ermöglichen. Um eine Verteilung zu verwenden, erstellen und hosten Sie zunächst Ihre Website oder Webanwendung auf einer Lightsail-Instance oder einem Containerservice oder mehreren Instances, die an einen Lightsail-Load Balancer angefügt sind oder speichern Sie Ihre statischen Inhalte auf einem Lightsail-Bucket. Anschließend erstellen und konfigurieren Sie eine Lightsail-Verteilung, um Inhalte aus Ihrer Instance, dem Containerservice, dem Load Balancer oder Ihrem Bucket abzurufen, zwischenzuspeichern und bereitzustellen. Ihre Instance, Ihr Containerservice, Ihren Load Balancer oder Ihr Bucket, auch bekannt als Ursprungsserver, ist die endgültige Quelle für Ihre Inhalte.

Wenn Ihr Benutzer Inhalte anfordert, indem er Ihre Website besucht, die über eine Verteilung bereitgestellt wird, wird die Anfrage in Bezug auf die Latenz an den nächstgelegenen Ort weitergeleitet. Anschließend führt die Verteilung eine der folgenden Aktionen durch:

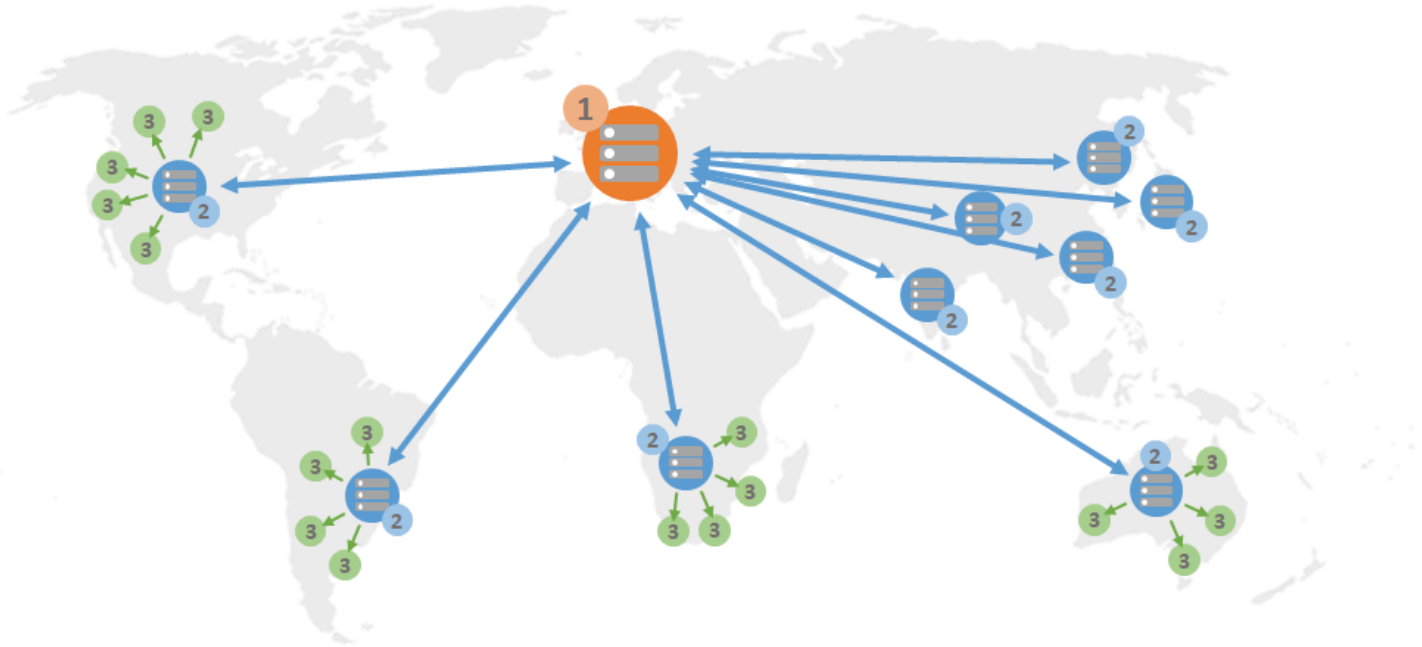
- Wenn der Inhalt bereits am Edge-Standort zwischengespeichert wird, werden sie von Ihrer Verteilung dem Benutzer sofort bereitgestellt.
- Wenn der Inhalt noch nicht an diesem Edge-Standort zwischengespeichert wird, ruft Ihre Verteilung ihn vom angegebenen Ursprung ab, speichert ihn zwischendurch und stellt ihn dem Benutzer zur Verfügung.

Ihre Inhalte werden an Edge-Standorten für die Dauer der Cache-Lebensdauer (Time to Live), die Sie für Ihre Verteilung angeben, zwischengespeichert, sodass andere Anforderungen am selben Speicherort sofort erfüllt werden. Der zwischengespeicherte Inhalt wird von der Edge-Position gelöscht, wenn er seine Cache-Lebensdauer erreicht. Ihre Verteilung ruft Inhalte ab, speichert sie und stellt sie bereit, wenn eine Inhaltsanforderung das nächste Mal an den Edge-Standort weitergeleitet wird.

In folgendem Diagramm:

- 1 stellt den Ursprung Ihrer Verteilung dar, z. B. Lightsail-Instance oder Containerservice, die Ihre Website hostet, einen Load Balancer mit angehängten Instances oder einen Bucket, der Ihre statischen Inhalte hostet.

- 2 stellt Ihre Verteilung oder die Edge-Positionen dar, die Inhalte aus Ihrem Ursprung abrufen, zwischenspeichern und bereitstellen.
- 3 stellt Ihre Benutzer dar, denen Inhalte von den Edge-Standorten bereitgestellt werden.

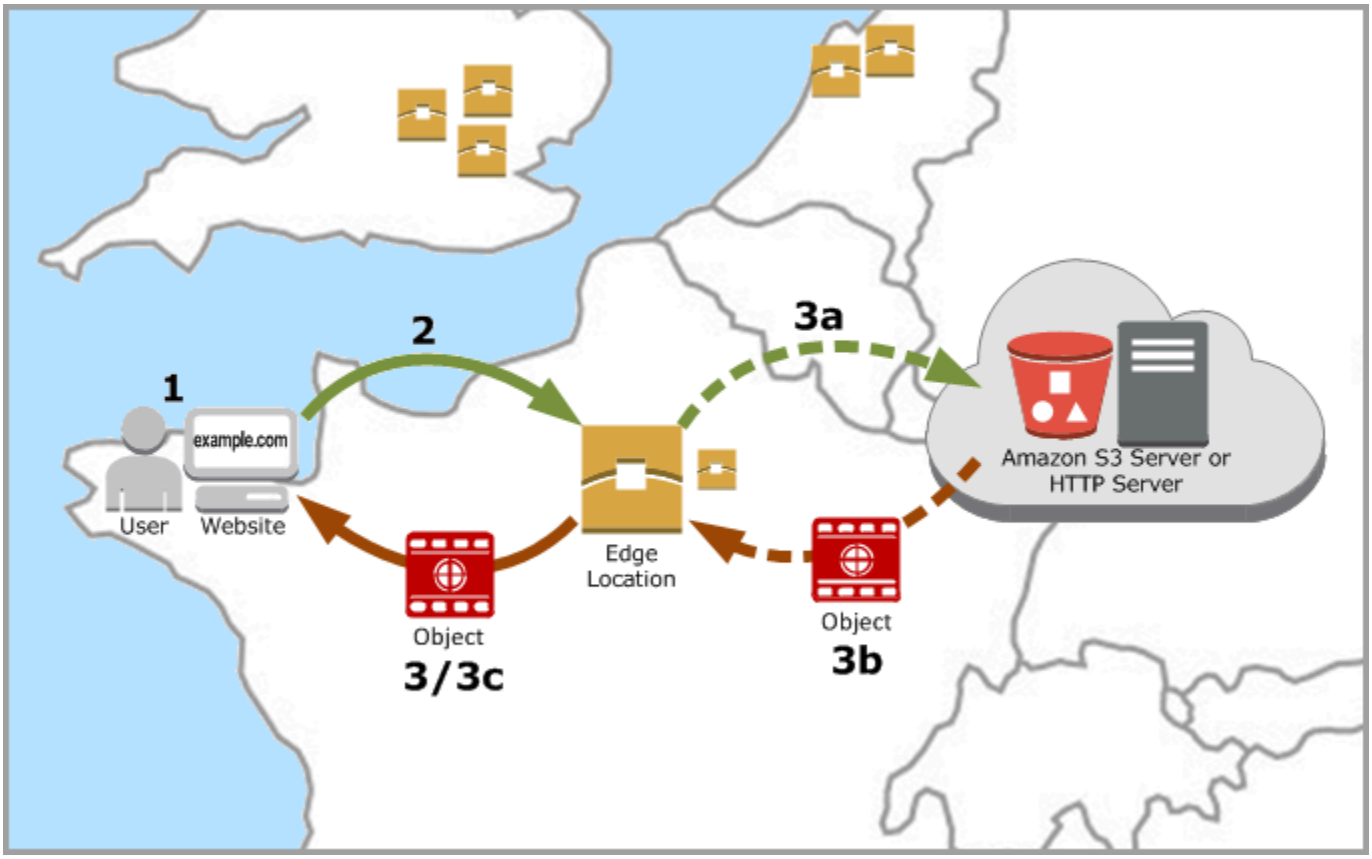


> **Note**
>
> Dieses Diagramm dient nur zur Veranschaulichung und zeigt keine tatsächlichen Edge-Standorte an. Weitere Informationen zu Edge-Positionen finden Sie unter Edge-Standorte und IP-Adressbereiche weiter unten in diesem Handbuch.

Wenn Ihre Website beispielsweise in Frankreich gehostet wird und eine Person aus einem anderen Gebiet Frankreichs Ihre Inhalte anzeigen möchte, wird die Seite in Millisekunden geladen.

Wenn Ihr Besucher nicht in der Nähe ist, wird es etwas schwierig.

Wenn eine Person aus Australien Ihre Inhalte anzeigen möchte, muss der Browser sie von einem Server abrufen, der sich in Frankreich befindet, und sie diesem Benutzer dann aus einer Entfernung von Tausenden Kilometern anzeigen. Wenn Benutzer aus verschiedenen Ländern denselben Inhalt zur gleichen Zeit anfordern, wird der Server mit Anfragen überlastet und braucht länger, um den Inhalt zu laden und bereitzustellen. Dies wirkt sich auf die Geschwindigkeit aus, mit der der Inhalt für den Endbenutzer geladen wird.



Ein CDN löst diese Situation, indem es Ihre Website-Inhalte an Edge-Standorten zwischenspeichert. Diese Art der Bereitstellung von Inhalten ist schneller und effizienter als die herkömmliche Methode, Inhalte aus einer zentralen Ressource bereitzustellen. Wenn ein Betrachter eine Anfrage auf Ihrer Website oder über Ihre Anwendung sendet, leitet DNS die Anfrage an den Standort weiter, der die Anforderung des Benutzers am besten bedienen kann. Ihre Benutzer greifen von Orten in der Nähe auf Ihre Inhalte zu, im Gegensatz dazu, dass alle Benutzer auf dieselbe zentrale Ressource zugreifen, die möglicherweise weit entfernt ist.

Anwendungsfälle

Bereitstellen schneller, sicherer Websites

Eine Lightsail-Verteilung beschleunigt die Bereitstellung Ihrer Inhalte (z. B. Websiteseiten, Bilder, Formatvorlagen, JavaScript usw.) für Betrachter weltweit. Durch die Verwendung einer Verteilung können Sie die Vorteile des AWS-Backbone-Netzwerks und der Edge-Server nutzen, um Ihren Betrachtern eine schnelle, sichere und zuverlässige Erfahrung zu bieten, wenn sie Ihre Website besuchen.

Verbessern der Sicherheit Ihrer Website

Stärken Sie Ihre Website und steigern Sie ihre Leistung, indem Sie die Vorteile der TLS-Terminierung nutzen, die die Belastung Ihres Origin-Servers reduziert, indem sie die kryptographische Verarbeitung auf Ihre Verteilung verlagert. Sie können Ihren registrierten Domainnamen zusammen mit einem Lightsail-SSL-/TLS-Zertifikat, um Hypertext Transfer Protocol Secure (HTTPS) für Ihre Verteilung zu aktivieren. Ihre Benutzer stellen eine verschlüsselte HTTPS-Verbindung zu Ihrer Verteilung her, während Ihre Verteilung mithilfe von HTTP Inhalte aus Ihrem Ursprung abruft.

Anwendungsoptimierung

Optimieren Sie Ihre Verteilungen ganz einfach für eine Vielzahl von Anwendungen, einschließlich WordPress und statischen Websites. Die Verwendung einer Verteilung zum Zwischenspeichern und Bereitstellen von Inhalten reduziert auch die Belastung Ihres Ursprungs, da die meisten Anforderungen von Ihrer Distribution und nicht von Ihrer Instance, Ihrem Containerservice, Ihrem Load Balancer-Service oder Ihrem Bucket bedient werden.

Konfigurieren der Verteilung

Dies sind die allgemeinen Schritte, die Sie befolgen müssen, um Ihre Website oder Webanwendung mithilfe eines Lightsail-Instance und eine Verteilung.

1. Vervollständigen Sie – je nachdem, ob Sie eine Instance, einen Containerservice oder einen Bucket mit Ihrer Verteilung verwenden möchten – einen der folgenden Schritte.

   - Erstellen Sie eine Lightsail-Instance, um Ihre Inhalte zu hosten. Die Instance dient als Ursprung Ihrer Verteilung. Auf einem Ursprungsserver sind die ursprünglichen, definitiven Versionen Ihres Inhalts gespeichert. Weitere Informationen finden Sie unter Erstellen einer Instance.

     Fügen Sie eine Lightsail statische IP Ihrer Instance hinzu. Die öffentliche Standard-IP-Adresse Ihrer Instance ändert sich, wenn Sie Ihre Instance stoppen und starten. Dadurch wird die Verbindung zwischen Ihrer Verteilung und Ihrer Ursprungsinstance unterbrochen. Eine statische IP ändert sich nicht, wenn Sie Ihre Instance anhalten und starten. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

     Laden Sie Ihre Inhalte und Dateien in Ihre Instance hoch. Ihre Dateien, auch als Objekte bezeichnet, enthalten normalerweise Webseiten, Bilder und Mediendateien, können jedoch alles sein, was über HTTP bereitgestellt werden kann.

- Erstellen Sie einen Lightsail-Containerservice zum Hosten Ihrer Website oder Webanwendung. Der Containerservice dient als Ursprung Ihrer Verteilung. Auf einem Ursprungsserver sind die ursprünglichen, definitiven Versionen Ihres Inhalts gespeichert. Weitere Informationen finden Sie unter Erstellen von Amazon Lightsail-Container-Services.
- Erstellen eines Lightsail-Bucket zur Speicherung Ihrer statischen Inhalte. Der Bucket dient als Ursprung Ihrer Verteilung. Auf einem Ursprungsserver sind die ursprünglichen, definitiven Versionen Ihres Inhalts gespeichert. Weitere Informationen finden Sie unter Einen Bucket erstellen.

  Laden Sie mithilfe der Lightsail-Konsole, AWS Command Line Interface (AWS CLI) und der AWS-APIs Dateien in Ihren Bucket hoch. Weitere Informationen zum Hochladen von Dateien finden Sie auf Hochladen von Dateien auf einen Bucket.

2. (Optional) Erstellen eines Lightsail-Load Balancers, wenn Ihre Website auf einer Instance gehostet wird, die Fehlertoleranz erfordert. Fügen Sie dann mehrere Kopien Ihrer Instance an den Load Balancer an. Sie können Ihren Load Balancer (mit einer oder mehreren angefügten Instances) als Ursprung Ihrer Verteilung konfigurieren, anstatt Ihre Instance als Ursprung zu konfigurieren. Weitere Informationen finden Sie unter Erstellen eines Load Balancers und Anfügen von Instances.
3. Erstellen Sie eine Lightsail-Verteilung und konfigurieren Sie Ihre Instance, Ihren Containerservice, Ihren Load-Balancer-Service oder Ihren Bucket als Ursprung. Gleichzeitig geben Sie Details wie die Cache-Lebensdauer Ihres Inhalts an und welche Elemente Ihrer Website oder Webanwendung zwischengespeichert werden. Weitere Informationen finden Sie unter Erstellen einer Verteilung.
4. (Optional) Falls der Ursprungsserver Ihrer Verteilung eine WordPress-Instance ist, müssen Sie die WordPress-Konfigurationsdatei in Ihrer Instance bearbeiten, damit Ihre WordPress-Website mit Ihrer Verteilung funktioniert. Weitere Informationen finden Sie unter Konfigurieren Ihrer WordPress-Instance für die Verwendung mit Ihrer Verteilung.
5. (Optional) Erstellen Sie eine Lightsail-DNS-Zone zur Verwaltung der DNS Ihrer Domäne in der Lightsail-Konsole. Auf diese Weise können Sie Ihre Domäne ganz einfach auf Ihre Lightsail-Ressourcen abbilden. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain. Alternativ können Sie weiterhin die DNS Ihrer Domäne hosten, wo sie derzeit gehostet wird.
6. Erstellen Sie ein Lightsail-SSL-/TLS-Zertifikat für Ihre Domain zur Verwendung mit Ihrer Verteilung. Lightsail-Verteilungen erfordern HTTPS, deshalb müssen Sie ein SSL-/TLS-Zertifikat für Ihre Domain anfordern, bevor Sie es mit Ihrer Verteilung verwenden können. Weitere Informationen finden Sie unter Erstellen von SSL-/TLS-Zertifikaten für Ihre Verteilung.

7. Aktivieren benutzerdefinierter Domains für Ihre Verteilungen, um Ihre registrierten Domainnamen mit Ihren Verteilungen zu verwenden. Das Aktivieren benutzerdefinierter Domänen erfordert, dass Sie das Lightsail-SSL-/TLS-Zertifikat, das Sie für Ihre Domäne erstellt haben, angeben. Dadurch werden Ihre Domänen zu Ihrer Verteilung hinzugefügt und HTTPS aktiviert. Weitere Informationen finden Sie unter Aktivieren benutzerdefinierter Domains für Ihre Verteilung.
8. Fügen Sie dem DNS Ihrer Domäne einen Aliasdatensatz hinzu, um zu beginnen, den Datenverkehr für Ihre Domäne an die Verteilung weiterzuleiten. Nachdem Sie die Aliasakte hinzugefügt haben, werden Benutzer, die Ihre Domäne besuchen, über Ihre Verteilung weitergeleitet. Weitere Informationen finden Sie unter Verweisen Ihrer Domain auf eine Verteilung.
9. Prüfen Sie, ob Ihre Verteilung Ihre Inhalte zwischenspeichert. Weitere Informationen finden Sie unter Testen Ihrer Verteilung.

Standorte und IP-Adressbereiche von -Edge-Servern

Lightsail-Verteilungen verwenden dieselben Edge-Server und IP-Adressbereiche wie Amazon CloudFront. Eine Liste der Standorte von CloudFront-Edge-Servern finden Sie auf der Amazon CloudFront-Produktdetailseite. Eine Liste der CloudFront-IP-Bereiche finden Sie in der Globalen IP-Liste von CloudFront.

Erstellen einer Netzwerkverteilung für die Bereitstellung von Inhalten in Lightsail

In diesem Handbuch zeigen wir Ihnen, wie Sie eine Amazon Lightsail-Verteilung mit der Lightsail-Konsole erstellen und die Verteilungseinstellungen beschreiben, die Sie konfigurieren können. Weitere Informationen zu Verteilungen finden Sie unter Netzwerkverteilungen für die Bereitstellung von Inhalten.

Inhalt

- Verzeichnis- und Dateiüberschreibungen
- Erweiterte Cache-Einstellungen
- Verteilungsplan
- Erstellen einer Verteilung
- Nächste Schritte

Voraussetzungen

Vervollständigen Sie die folgenden Voraussetzungen, bevor Sie mit dem Erstellen einer Verteilung beginnen:

1. Vervollständigen Sie – je nachdem, ob Sie eine Instance, einen Containerservice oder einen Bucket mit Ihrer Verteilung verwenden möchten – einen der folgenden Schritte.
   - Erstellen Sie eine Lightsail-Instance, um Ihre Inhalte zu hosten. Die Instance dient als Ursprung Ihrer Verteilung. Auf einem Ursprungsserver sind die ursprünglichen, definitiven Versionen Ihres Inhalts gespeichert. Weitere Informationen finden Sie unter Erstellen einer Instance.

     Fügen Sie Ihrer Instance eine statische Lightsail-IP an. Die öffentliche Standard-IP-Adresse Ihrer Instance ändert sich, wenn Sie Ihre Instance stoppen und starten. Dadurch wird die Verbindung zwischen Ihrer Verteilung und Ihrer Ursprungsinstance unterbrochen. Eine statische IP ändert sich nicht, wenn Sie Ihre Instance anhalten und starten. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

     Laden Sie Ihre Inhalte und Dateien in Ihre Instance hoch. Ihre Dateien, auch als Objekte bezeichnet, enthalten normalerweise Webseiten, Bilder und Mediendateien, können jedoch alles sein, was über HTTP bereitgestellt werden kann.
   - Erstellen Sie einen Lightsail-Container-Service, um Ihre Website oder Webanwendung zu hosten. Der Containerservice dient als Ursprung Ihrer Verteilung. Auf einem Ursprungsserver sind die ursprünglichen, definitiven Versionen Ihres Inhalts gespeichert. Weitere Informationen finden Sie unter Erstellen von Amazon-Lightsail-Container-Servicesn.
   - Erstellen Sie einen Lightsail-Bucket, um Ihre statischen Inhalte zu speichern. Der Bucket dient als Ursprung Ihrer Verteilung. Auf einem Ursprungsserver sind die ursprünglichen, definitiven Versionen Ihres Inhalts gespeichert. Weitere Informationen finden Sie unter Einen Bucket erstellen.

Laden Sie Dateien mithilfe der Lightsail-Konsole, der AWS Command Line Interface (AWS CLI) und der AWS APIs in Ihren Bucket hoch. Weitere Informationen zum Hochladen von Dateien finden Sie auf Hochladen von Dateien auf einen Bucket.

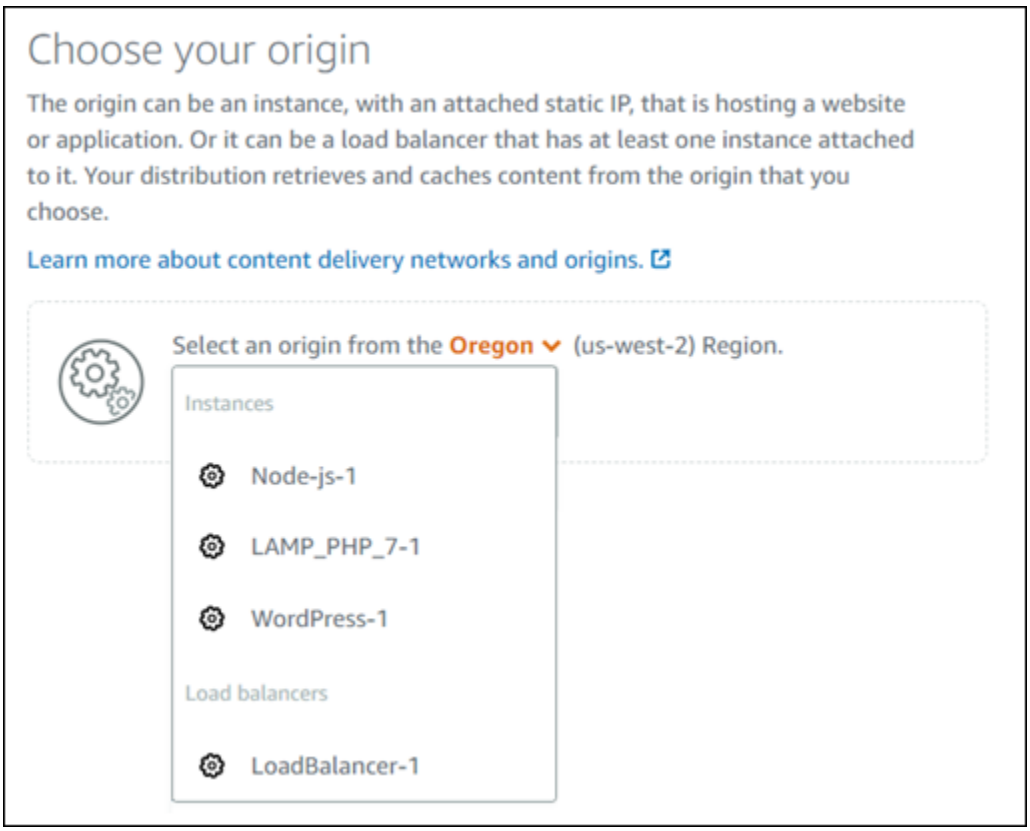
2. (Optional) Erstellen Sie einen Lightsail Load Balancer, wenn Ihre Website Fehlertoleranz erfordert. Fügen Sie dann mehrere Kopien Ihrer Instance an den Load Balancer an. Sie können Ihren Load Balancer (mit einer oder mehreren angefügten Instances) als Ursprung Ihrer Verteilung konfigurieren, anstatt Ihre Instance als Ursprung zu konfigurieren. Weitere Informationen finden Sie unter Erstellen eines Load Balancers und Anfügen von Instances.

Ursprungs-Ressource

Ein Ursprungsserver ist die definitive Quelle von Inhalten für Ihre Verteilung. Wenn Sie Ihre Verteilung erstellen, wählen Sie die Lightsail-Instance, den Container-Service, den Bucket oder den Load Balancer (mit einer oder mehreren angefügten Instances), die den Inhalt Ihrer Website oder Webanwendung hostet.

> **Note**
>
> IPv6-onlyInstances können derzeit nicht als Ursprung für eine Lightsail Content Delivery Network (CDN)-Verteilung konfiguriert werden.

Sie können nur einen Ursprungsserver pro Verteilung auswählen. Sie können den Ursprungsserver jederzeit ändern, nachdem Sie Ihre Verteilung erstellt haben. Weitere Informationen finden Sie unter Ändern des Ursprungs Ihrer Verteilung.



Ursprungsprotokollrichtlinie

Die Ursprungsprotokollrichtlinie ist die Protokollrichtlinie, die Ihre Verteilung beim Abrufen von Inhalten aus Ihrem Ursprungsserver verwendet. Nachdem Sie einen Ursprungsserver für Ihre Verteilung ausgewählt haben, sollten Sie festlegen, ob Ihre Verteilung Hypertext Transfer Protocol (HTTP) oder Hypertext Transfer Protocol Secure (HTTPS) verwenden soll, wenn Inhalte aus Ihrem Ursprungsserver abgerufen werden. Wenn Ihr Ursprungsserver nicht für HTTPS konfiguriert ist, müssen Sie HTTP verwenden.

Sie können für Ihre Verteilung eine der folgenden Ursprungs-Protokollrichtlinien auswählen:

- Nur HTTP - Ihre Verteilung verwendet nur HTTP für den Zugriff auf den Ursprungsserver. Dies ist die Standardeinstellung.
- Nur HTTPS - Ihre Verteilung verwendet nur HTTPS für den Zugriff auf den Ursprungsserver.

Die Schritte zum Bearbeiten der Ursprungsprotokollrichtlinie sind im Abschnitt Eine Verteilung erstellen an späterer Stelle in diesem Leitfaden.

> **Note**
>
> Wenn Sie einen Lightsail-Bucket als Ursprung Ihrer Verteilung auswählen, verwendet die Ursprungsprotokollrichtlinie standardmäßig nur HTTPS. Sie können die Ursprungsprotokollrichtlinie nicht ändern, wenn einen Bucket der Ursprungsserver Ihrer Verteilung ist.

Caching-Verhalten und Caching-Voreinstellungen

Eine Caching-Voreinstellungkonfiguriert automatisch die Einstellungen Ihrer Verteilung für den Inhaltstyp, den Sie auf Ihrem Ursprungsserver hosten. Wählen Sie zum Beispiel die OptionOptimal für statische Inhalte, konfiguriert Ihre Verteilung automatisch mit Einstellungen, die für statische Websites am besten geeignet sind. Wenn Ihre Website auf einer WordPress Instance gehostet wird, wählen Sie die Option Optimal für WordPress die Voreinstellung, damit Ihre Verteilung automatisch für die Arbeit mit Ihrer WordPress Website konfiguriert wird.

> **Note**
>
> Die Optionen für die Caching-Voreinstellung sind nicht verfügbar, wenn Sie einen Lightsail-Bucket als Ursprung Ihrer Verteilung auswählen. Wir wenden automatisch Verteilungseinstellungen an, die sich am besten für statische Inhalte eignen, die in einem Bucket gespeichert werden.

Sie können für Ihre Verteilung eine der folgenden Caching-Voreinstellungen auswählen:

- Optimal für statische Inhalte- Diese Voreinstellung konfiguriert Ihre Verteilung aufAlles cachen. Diese Voreinstellung ist ideal, wenn Sie statische Inhalte (z. B. statische HTML-Seiten) auf Ihrem Ursprungsserver hosten, oder Inhalte, die sich nicht für jeden Benutzer ändern, der Ihre Website besucht. Alle Inhalte in Ihrer Verteilung werden gecached, wenn Sie diese Voreinstellung auswählen.
- Optimal für dynamische Inhalte – Diese Voreinstellung konfiguriert Ihre Verteilung so, dass nichts außer den angegebenen Dateien gecached wird, die Sie als Cache im Abschnitt Verzeichnis- und Dateiüberschreibungen auf der Seite Eine Verteilung erstellen angeben. Weitere Informationen finden Sie unter Verzeichnis- und Dateiüberschreibungen weiter unten in diesem Leitfaden. Diese Voreinstellung ist ideal, wenn Sie dynamische Inhalte zu Ihrem Ursprungsserver hosten

oder Inhalte, die sich für jeden Benutzer ändern können, der Ihre Website oder Webanwendung besucht.

- Optimal für WordPress – Diese Voreinstellung konfiguriert Ihre Verteilung so, dass nichts zwischengespeichert wird, außer die Dateien in den `wp-content/` Verzeichnissen `wp-includes/` und Ihrer WordPress Instance. Diese Voreinstellung ist ideal, wenn Ihr Ursprung eine Instance ist, die den Blueprint WordPress Certified by Bitnami und Automattic verwendet (mit Ausnahme des Multisite-Blueprints). Weitere Informationen zu dieser Voreinstellung finden Sie unter Optimal für WordPress die Caching-Voreinstellung .

> **Note**
>
> Die Voreinstellung Benutzerdefinierte Einstellungen kann nicht ausgewählt werden. Es wird automatisch für Sie ausgewählt, wenn Sie eine Voreinstellung auswählen, dann aber die Einstellungen Ihrer Verteilung manuell ändern.

Eine Caching-Voreinstellung kann nur in der Lightsail-Konsole angegeben werden. Sie kann nicht mit der Lightsail-API, AWS CLIund SDKs angegeben werden.

Optimal für WordPress die Caching-Voreinstellung

Wenn Sie eine Instance auswählen, die den Blueprint WordPress Certified by Bitnami und Automattic als Ursprung Ihrer Verteilung verwendet, fragt Lightsail, ob Sie die Voreinstellung Best for WordPress Caching auf Ihre Verteilung anwenden möchten. Wenn Sie die vorhandene anwenden, wird Ihre Verteilung automatisch so konfiguriert, dass sie am besten mit Ihrer WordPress Website funktioniert. Es gibt keine anderen Verteilungseinstellungen, die Sie anwenden müssen. Die beste für die WordPress Voreinstellung, um nichts außer den Dateien in den Verzeichnissen und Ihrer Website zwischenzuspeichern. `wp-includes/` `wp-content/` WordPress Es konfiguriert auch Ihre Verteilung, um ihren Cache jeden Tag zu löschen (Cache-Lebensdauer von 1 Tag), alle HTTP-Methoden zuzulassen, nur die`Host`Kopfzeile, keine Cookies und alle Abfragezeichenfolgen weiterzuleiten.

> **Important**
>
> Sie müssen die WordPress Konfigurationsdatei in Ihrer Instance bearbeiten, damit Ihre WordPress Website mit Ihrer Verteilung funktioniert. Weitere Informationen finden Sie unter Konfigurieren Ihrer WordPress Instance für die Arbeit mit Ihrer Verteilung.

Standardverhalten

Ein Standardverhaltengibt an, wie Ihre Verteilung das Inhalt-Caching verarbeitet. Das Standardverhalten Ihrer Verteilung wird automatisch für Sie festgelegt, abhängig von derCaching-Voreinstellung, die Sie auswählen. Wenn Sie ein anderes Standardverhalten auswählen, wird die Caching-Voreinstellung automatisch inBenutzerdefinierte Einstellungengeändert.

> **Note**
>
> Die Standardverhaltensoptionen sind nicht verfügbar, wenn Sie einen Lightsail-Bucket als Ursprung Ihrer Verteilung auswählen. Wir wenden automatisch Verteilungseinstellungen an, die sich am besten für statische Inhalte eignen, die in einem Bucket gespeichert werden.

Sie können für Ihre Verteilung eine der folgenden Standardverhalten auswählen:

- Alles cachen- Durch dieses Verhalten wird Ihre Verteilung so konfiguriert, dass sie Ihre gesamte Website als statischer Inhalt zwischenspeichert und bereitgestellt wird. Diese Option ist ideal, wenn Ihr Ursprungsserver Inhalte hostet, die sich je nachdem, wer sie ansieht, nicht ändert, oder wenn Ihre Website keine Cookies, Kopfzeilen oder Abfragezeichenfolgen verwendet, um Inhalte zu personalisieren.
- Nichts cachen- Dieses Verhalten konfiguriert Ihre Verteilung so, dass nur die von Ihnen angegebenen Ursprungsdateien und Ordnerpfade gecached werden. Diese Option ist ideal, wenn Ihre Website oder Webanwendung Cookies, Kopfzeilen und Abfragezeichenfolgen verwendet, um Inhalte für einzelne Benutzer zu personalisieren. Wenn Sie diese Option auswählen, müssenSie die Verzeichnis- und Dateipfadüberschreibungen zum cachen angeben.

Verzeichnis- und Dateiüberschreibungen

EineVerzeichnis- und Dateiüberschreibungkann verwendet werden, um das von Ihnen ausgewählte Standardverhalten zu überschreiben oder eine Ausnahme hinzuzufügen. Wenn Sie beispielsweiseAlles cachen wählen, verwenden Sie eine Überschreibung, um ein Verzeichnis, eine Datei oder einen Dateityp anzugeben, den Ihre Verteilung nicht cachen soll. Wenn Sie alternativ Nichts cachen wählen, verwenden Sie eine Überschreibung, um ein Verzeichnis, eine Datei oder einen Dateityp anzugeben, den Ihre Verteilung cachen soll.

In dem Abschnitt Verzeichnis- und Dateiüberschreibungen der Seite können Sie einen Pfad zu einem Verzeichnis oder einer Datei angeben, die zwischengespeichert werden soll

oder nicht zwischengespeichert werden soll. Verwenden Sie ein Sternchen-Symbol, um Platzhalterverzeichnisse (`path/to/assets/*`) und Dateitypen (`*.html`, `*jpg`, `*js`) anzugeben. Bei Verzeichnissen und Dateien muss die Groß- und Kleinschreibung beachtet werden.

> **Note**
>
> Die Verzeichnis- und Dateiüberschreibungsoptionen sind nicht verfügbar, wenn Sie einen Lightsail-Bucket als Ursprung Ihrer Verteilung auswählen. Alles, was im ausgewählten Bucket gespeichert ist, wird gecached.

Dies sind nur einige Beispiele, wie Sie Verzeichnis- und Dateiüberschreibungen angeben können:

- Geben Sie Folgendes an, um alle Dateien im Dokumentenstamm eines Apache-Webservers zwischenzuspeichern, der auf einer Lightsail-Instance ausgeführt wird.

  ```
  var/www/html/
  ```

- Geben Sie die folgende Datei an, um nur die Index-Seite im Dokumentenstamm eines Apache-Webservers zu cachen.

  ```
  var/www/html/index.html
  ```

- Geben Sie Folgendes an, um nur die .html-Dateien im Dokumentenstamm eines Apache-Webservers zu cachen.

  ```
  var/www/html/*.html
  ```

- Geben Sie Folgendes an, um nur die .jpg,- .png- und .gif-Dateien im Images-Unterverzeichnis des Dokumentstamms eines Apache-Webservers zu cachen.

  ```
  var/www/html/images/*.jpg
  ```

  ```
  var/www/html/images/*.png
  ```

  ```
  var/www/html/images/*.gif
  ```

Geben Sie Folgendes an, um alle Dateien im Images-Unterverzeichnis des Dokumentstamms eines Apache-Webservers zu cachen.

```
var/www/html/images/
```

Erweiterte Cache-Einstellungen

DieErweiterte Einstellungenkönnen verwendet werden, um die Cache-Lebensdauer von Inhalten in Ihrer Verteilung, die zulässigen HTTP-Methoden, die HTTP-Kopfzeilenweiterleitung, die Cookie-Weiterleitung und die Weiterleitung von Abfragezeichenfolgen, anzugeben. Die erweiterten Einstellungen, die Sie angeben, gelten nur für das Verzeichnis und die Dateien, die Ihre Verteilung zwischenspeichert, einschließlich der Verzeichnis- und Dateiüberschreibungen, die Sie als Cache angeben.

> **Note**
>
> Die erweiterten Cache-Einstellungen sind auf der Seite Verteilung erstellen nicht verfügbar, wenn Sie einen Lightsail-Bucket als Ursprung Ihrer Verteilung auswählen. Wir wenden automatisch Verteilungseinstellungen an, die sich am besten für statische Inhalte eignen, die in einem Bucket gespeichert werden. Sie können jedoch die erweiterten Cache-Einstellungen auf der Seite für die Verteilungsverwaltung ändern, nachdem Ihre Verteilung erstellt wurde.

Sie können die folgenden erweiterten Einstellungen konfigurieren:

Cache-Lebensdauer (TTL)

Steuert die Zeitspanne, in der Ihre Inhalte im Cache Ihrer Verteilung bleiben, bevor Ihre Verteilung eine weitere Anforderung an Ihren Ursprungsserver weiterleitet, um zu ermitteln, ob Ihre Inhalte aktualisiert wurden. Der Standardwert beträgt einen Tag. Eine Reduzierung der Dauer ermöglicht Ihnen, dynamische Inhalte besser bereitzustellen. Eine Erhöhung der Dauer bedeutet, dass Ihre Benutzer eine bessere Leistung erhalten, da es wahrscheinlicher ist, dass Ihre Dateien direkt vom Edge-Standort bereitgestellt werden. Eine Erhöhung der Dauer verringert darüber hinaus die Last auf Ihrem Ursprungsserver, da Ihre Verteilung weniger häufig Inhalte abruft.

> **Note**
>
> Der angegebene Wert der Cache-Lebensdauer gilt nur, wenn Ihr Ursprungsserver keine HTTP-Kopfzeilen, wie z. B. `Cache-Control max-age`, `Cache-Control s-maxage` oder `Expires` hinzufügt.

Zulässige HTTP-Methoden

Steuert die HTTP-Methoden, die Ihre Verteilung verarbeitet und an Ihren Ursprungsserver weiterleitet. HTTP-Methoden verweisen auf die gewünschte Tätigkeit, die auf dem Ursprungsserver ausgeführt werden soll. Die GET-Methode ruft beispielsweise Daten von Ihrem Ursprungsserver ab, und die PUT-Methode fordert an, dass die abgeschlossene Einheit auf Ihrem Ursprungsserver gespeichert wird.

Sie können für Ihre Verteilung eine der folgenden Optionen für HTTP-Methoden auswählen:

- HTTP-Methoden GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE erlauben
- Erlauben der GET-, HEAD- und OPTI-Methoden
- Erlauben der GET- und HEAD-Methoden

Ihre Verteilung speichert immer Antworten auf die GET- und HEAD-Anforderungen zwischen. Ihre Verteilung speichert auch Antworten auf die OPTIONS-Anforderungen zwischen, wenn Sie diese Anforderungen erlauben. Ihre Verteilung speichert keine Antworten auf andere HTTP-Methoden zwischen. Weitere Informationen finden Sie unter HTTP-Methoden.

> **Important**
>
> Wenn Sie Ihre Verteilung so konfigurieren, dass alle HTTP-Methoden zulässig sind, die unterstützt werden, müssen Sie Ihre Ursprung-Instance so konfigurieren, dass alle Methoden verarbeitet werden. Wenn Sie beispielsweise Ihre Verteilung so konfigurieren, dass diese Methoden zulässig sind, weil Sie POST verwenden möchten, müssen Sie Ihren Ursprungsserver so konfigurieren, dass er DELETE-Anforderungen entsprechend erledigen kann, damit Viewer keine Ressourcen löschen können, von denen Sie nicht wünschen, dass diese gelöscht werden. Beziehen Sie sich für weitere Informationen auf die Unterlagen für Ihre Website oder Webanwendung.

Weiterleiten der HTTP-Kopfzeile

Steuert, ob Ihre Verteilung den Inhalt, basierend auf den Werten der angegebenen Kopfzeilen, zwischenspeichert und wenn ja, welche. HTTP-Kopfzeilen enthalten Informationen über den Client-Browser, der angeforderten Seite, den Ursprung und mehr. Zum Beispiel sendet der `Accept-Language`-Header die Sprache des Kunden (beispielsweise `en-US` für Englisch), so dass der Ursprung mit Inhalten in der Sprache des Kunden antworten kann, falls diese verfügbar ist.

Sie können für Ihre Verteilung eine der folgenden HTTP-Kopfzeilen-Optionen auswählen:

- Kein Weiterleiten von Kopfzeilen
- Nur Kopfzeilen weiterleiten, die ich angebe

Wenn SieKein Weiterleiten von Kopfzeilenwählen, speichert Ihre Verteilung den Inhalt nicht basierend auf Kopfzeilenwerten zwischen. Unabhängig von der von Ihnen gewählten Option, leitet Ihre Verteilung bestimmte Kopfzeilen an Ihren Ursprungsserver weiter und führt spezifische Tätigkeiten basierend auf den von Ihnen weitergeleiteten Kopfzeilen aus. Weitere Informationen darüber, wie Ihre Verteilung die Weiterleitung von Kopfzeilen verarbeitet, finden Sie unterAnforderungen von HTTP-Kopfzeilen und Verteilungsverhalten.

Weiterleiten von Cookies

Steuert, ob Ihre Verteilung Cookies an Ihren Ursprungsserver weiterleitet und gegebenenfalls welche. Ein Cookie enthält einen kleinen Anteil von Daten, die an den Ursprungsserver gesendet werden, wie Informationen über die Tätigkeit eines Besuchers auf einer Webseite Ihrer Herkunft, sowie alle Informationen, die der Besucher zur Verfügung gestellt hat, wie etwa seinen Namen und Interessen.

Sie können für Ihre Verteilung eine der folgenden Cookie-Weiterleitung-Optionen auswählen:

- Keine Cookies weiterleiten
- Alle Cookies weiterleiten
- Nur Cookies weiterleiten, die ich angebe

Wenn Sie Alle weiterleiten wählen, leitet Ihre Verteilung alle Cookies weiter, unabhängig davon, wie viele Ihre Anwendung verwendet. Wenn Sie Cookies weiterleiten, die ich bestimme wählen, dann geben Sie die Namen der Cookies ein, die Ihre Verteilung weiterleiten soll, in das angezeigte Textfeld ein. Sie können die folgenden Platzhalter spezifizieren, wenn Sie Cookie-Namen angeben:

- * steht für 0 oder mehr Zeichen in dem Cookie-Namen

- ? steht für genau 1 Zeichen in dem Cookie-Namen

Nehmen wir beispielsweise an, dass Viewer-Anfragen für ein Objekt ein Cookie mit dem Namen `userid_`*`member-number`* beinhaltet. Dabei hat jeder Ihrer Benutzer einen eindeutigen Wert für `member-number` (`userid_123`, `userid_124`, `userid_125`). Sie möchten, dass Ihre Verteilung eine separate Version des Inhalts für jedes Mitglied zwischenspeichert. Sie könnten dies erreichen, indem Sie alle Cookies an Ihren Ursprungsserver weiterleiten. Viewer-Anfragen enthalten jedoch einige Cookies, die Sie nicht von Ihrer Verteilung zwischengespeichert haben möchten. Alternativ könnten Sie den folgenden Wert als Cookie-Namen angeben, was bewirkt, dass Ihre Verteilung alle Cookies, die mit `userid_` beginnen, an Ihren Ursprungsserver `userid_*` weiterleiten:

Weiterleiten einer Abfragezeichenfolge

Steuert, ob Ihre Verteilung Abfragezeichenfolgen an Ihren Ursprungsserver weiterleitet und gegebenenfalls welche. Eine Abfragezeichenfolge ist ein Teil einer URL, die den angegebenen Parametern Werte zuweist. Zum Beispiel beinhaltet die`https://example.com/over/there?name=ferret` URL die`name=ferret` Abfragezeichenfolge. Wenn ein Server eine Anforderung für eine solche Seite erhält, kann er ein Programm ausführen, das die`name=ferret`-Abfragezeichenfolge unverändert an das Programm weitergibt. Das Fragezeichen wird als Trennzeichen verwendet und ist nicht Teil der Abfragezeichenfolge.

Sie können festlegen, dass Ihre Verteilung keine Abfragezeichenfolgen weiterleitet oder nur die von Ihnen angegebenen. Wählen Sie diese Option aus, um Abfragezeichenfolgen nicht weiterleiten zu lassen, wenn Ihr Ursprungsserver dieselbe Version Ihres Inhalts unabhängig von den Werten der Abfragezeichenfolge-Parameter zurückgibt. Dies erhöht die Wahrscheinlichkeit, dass Ihre Verteilung eine Anfrage vom Cache bereitstellen kann, wodurch die Leistung verbessert und die Last auf Ihrem Ursprungsserver reduziert wird. Wählen Sie diese Option aus, um Abfragezeichenfolgen, die Sie angeben, weiterleiten zu lassen, wenn Ihr Ursprungsserver verschiedene Versionen Ihres Inhalts auf der Grundlage von einem oder mehreren Abfragezeichenfolge-Parametern zurückgibt.

Verteilungsplan

EinVerteilungsplangibt das monatliche Datenübertragungskontingent und die Kosten für Ihre Verteilung an. Wenn Ihre Verteilung mehr Daten überträgt als das monatliche Datenübertragungskontingent Ihres Plans, wird Ihnen eine Überschreitung in Rechnung gestellt. Weitere Informationen finden Sie in der Lightsail-Preisliste.

Um eine Überschreitungsgebühr zu vermeiden, ändern Sie den aktuellen Plan Ihrer Verteilung in einen anderen Plan, der eine größere Menge an monatlichen Datenübertragungen bietet, bevor

Ihre Verteilung das monatliche Kontingent überschreitet. Sie können Ihren Verteilungsplan nur einmal während jedes AWS-Abrechnungszeitraums ändern. Weitere Informationen zum Ändern des Verteilungsplans nach dem Erstellen, finden Sie unter Ändern des Plans Ihrer Verteilung.

Eine Verteilung erstellen

Vervollständigen Sie das folgende Verfahren, um einen Verteilung zu erstellen.

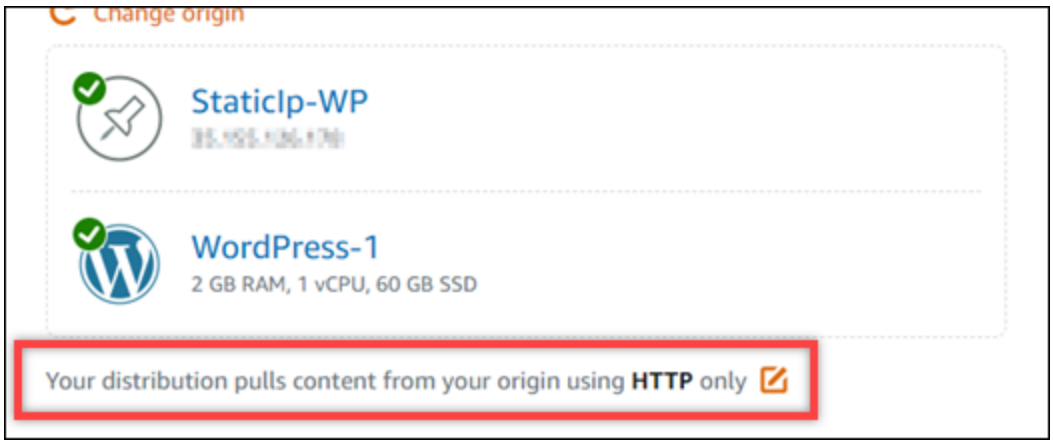
1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Networking (Netzwerk).
3. Wählen Sie Verteilung erstellen aus.
4. In dem Abschnitt Wählen Sie Ihren Ursprung der Seite, wählen Sie die AWS-Region, in dem Ihre Ursprungs-Ressource erstellt wurde.

   Verteilungen sind globale Ressourcen. Sie können auf einen Ursprung in jeder AWS-Region verweisen, und den Inhalt global verteilen.
5. Wählen Sie Ihren Ursprungsserver aus. Ein Ursprung kann eine Lightsail-Instance, ein Container-Service, ein Bucket oder ein Load Balancer (mit einer oder mehreren angefügten Instances) sein. Weitere Informationen finden Sie unter Ursprungsserver-Ressourcen.

   > **Important**
   >
   > Wenn Sie einen Lightsail-Container-Service als Ursprung Ihrer Verteilung wählen, fügt Lightsail automatisch den Standarddomänennamen Ihrer Verteilung als benutzerdefinierte Domäne zu Ihrem Container-Service hinzu. Auf diese Weise kann der Datenverkehr zwischen Ihrer Verteilung und Ihrem Containerservice geleitet werden. Es gibt jedoch einige Umstände, unter denen Sie möglicherweise den Standard Domainnamen Ihrer Verteilung manuell zu Ihrem Containerservice hinzufügen müssen. Weitere Informationen finden Sie unter Hinzufügen der Standard-Domain einer Verteilung zu einem Container-Service.
6. (Optional) Um die Ursprungsprotokollrichtlinie zu ändern, wählen Sie das Stiftsymbol, das neben der aktuellen Ursprungsprotokollrichtlinie angezeigt wird, die Ihre Verteilung verwendet. Weitere Informationen finden Sie unter Ursprungsprotokollrichtlinie.

   Diese Option ist im Abschnitt Wählen Sie Ihren Ursprungsserver der Seite unter den Ursprungs-Ressource aufgeführt, die Sie für Ihre Verteilung ausgewählt haben.

> **Note**
>
> Wenn Sie einen Lightsail-Bucket als Ursprung Ihrer Verteilung auswählen, verwendet die Ursprungsprotokollrichtlinie standardmäßig nur HTTPS. Sie können die Ursprungsprotokollrichtlinie nicht ändern, wenn einen Bucket der Ursprungsserver Ihrer Verteilung ist.



7. Wählen Sie das Caching-Verhalten (auch Caching-Voreinstellung genannt) für Ihre Verteilung aus. Weitere Informationen finden Sie unterCaching-Verhalten und Caching-Voreinstellung.

> **Note**
>
> Die Optionen für die Caching-Voreinstellung sind nicht verfügbar, wenn Sie einen Lightsail-Bucket als Ursprung Ihrer Verteilung auswählen. Wir wenden automatisch Verteilungseinstellungen an, die sich am besten für statische Inhalte eignen, die in einem Bucket gespeichert werden.

8. (Optional) Wählen Sie Anzeigen aller Einstellungen, um zusätzliche Einstellungen für das Caching-Verhalten für Ihre Verteilung anzuzeigen.

> **Note**
>
> Die Einstellungen für das Caching-Verhalten sind nicht verfügbar, wenn Sie einen Lightsail-Bucket als Ursprung Ihrer Verteilung auswählen. Wir wenden automatisch

Verteilungseinstellungen an, die sich am besten für statische Inhalte eignen, die in einem Bucket gespeichert werden.

9. (Optional) Wählen Sie das Standardverhalten für Ihre Verteilung aus. Weitere Informationen finden Sie unter Standardverhalten.

> **Note**
>
> Die Standardverhaltensoptionen sind nicht verfügbar, wenn Sie einen Lightsail-Bucket als Ursprung Ihrer Verteilung auswählen. Wir wenden automatisch Verteilungseinstellungen an, die sich am besten für statische Inhalte eignen, die in einem Bucket gespeichert werden.

10. (Optional) Wählen Sie Pfad hinzufügen, um ein Verzeichnis und eine Dateiüberschreibung zum Caching-Verhalten Ihrer Verteilung hinzuzufügen. Weitere Informationen finden Sie unter Verzeichnis- und Dateiüberschreibungen.

> **Note**
>
> Die Verzeichnis- und Dateiüberschreibungsoptionen sind nicht verfügbar, wenn Sie einen Lightsail-Bucket als Ursprung Ihrer Verteilung auswählen. Wir wenden automatisch Verteilungseinstellungen an, die sich am besten für statische Inhalte eignen, die in einem Bucket gespeichert werden.

11. (Optional) Wählen Sie das Stiftsymbol aus, das neben der erweiterten Einstellung angezeigt wird, die Sie für Ihre Verteilung bearbeiten möchten. Weitere Informationen finden Sie unter Erweiterte Cache-Einstellungen.

> **Note**
>
> Die erweiterten Cache-Einstellungen sind auf der Seite Verteilung erstellen nicht verfügbar, wenn Sie einen Lightsail-Bucket als Ursprung Ihrer Verteilung auswählen. Wir wenden automatisch Verteilungseinstellungen an, die sich am besten für statische Inhalte eignen, die in einem Bucket gespeichert werden. Sie können jedoch die erweiterten Cache-Einstellungen auf der Seite für die Verteilungsverwaltung ändern, nachdem Ihre Verteilung erstellt wurde.

12. Wählen Sie Ihren Verteilungsplan aus. Weitere Informationen finden Sie unter Verteilungspläne.

13. Geben Sie einen Namen für Ihre Verteilung ein.

    Ressourcennamen:

    - Muss in jedem AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
    - Muss zwischen 2 und 255 Zeichen enthalten.
    - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
    - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.
14. Überprüfen Sie die Kosten für Ihre Verteilung.
15. Wählen Sie Verteilung erstellen aus.

    Ihre Verteilung wird nach wenigen Augenblicken erstellt.

Nächste Schritte

Wir empfehlen, dass Sie die folgenden Schritte ausführen, nachdem Ihre Verteilung betriebsbereit ist.

1. Wenn der Ursprung Ihrer Verteilung eine WordPress Instance ist, müssen Sie die WordPress Konfigurationsdatei in Ihrer Instance bearbeiten, damit Ihre WordPress Website mit Ihrer Verteilung funktioniert. Weitere Informationen finden Sie unter Konfigurieren Ihrer WordPress Instance für die Arbeit mit Ihrer Verteilung.
2. (Optional) Erstellen Sie eine Lightsail-DNS-Zone, um den DNS Ihrer Domain in der Lightsail-Konsole zu verwalten. Auf diese Weise können Sie Ihre Domain einfach Ihren Lightsail-Ressourcen zuordnen. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain. Alternativ können Sie weiterhin die DNS Ihrer Domäne hosten, wo sie derzeit gehostet wird.
3. Erstellen Sie ein Lightsail-SSL-/TLS-Zertifikat für Ihre Domain, um es mit Ihrer Verteilung zu verwenden. Lightsail-Verteilungen erfordern HTTPS, daher müssen Sie ein SSL-/TLS-Zertifikat für Ihre Domäne anfordern, bevor Sie es mit Ihrer Verteilung verwenden können. Weitere Informationen finden Sie unter Erstellen von SSL-/TLS-Zertifikaten für Ihre Verteilung.
4. Aktivieren Sie benutzerdefinierte Domänen für Ihre Verteilung, um Ihre Domäne mit Ihrer Verteilung zu verwenden. Um benutzerdefinierte Domänen zu aktivieren, müssen Sie das Lightsail-SSL-/TLS-Zertifikat angeben, das Sie für Ihre Domäne erstellt haben. Dadurch wird Ihre Domain zur Verteilung hinzugefügt und HTTPS aktiviert. Weitere Informationen finden Sie unter Aktivieren benutzerdefinierter Domains für Ihre Verteilung.

5. Fügen Sie dem DNS Ihrer Domäne einen Aliasdatensatz hinzu, um zu beginnen, den Datenverkehr für Ihre Domäne an die Verteilung weiterzuleiten. Nachdem Sie die Aliasakte hinzugefügt haben, werden Benutzer, die Ihre Domäne besuchen, über Ihre Verteilung weitergeleitet. Weitere Informationen finden Sie unter Verweisen Ihrer Domain auf eine Verteilung.
6. Prüfen Sie, ob Ihre Verteilung Ihre Inhalte zwischenspeichert. Weitere Informationen finden Sie unter Testen Ihrer Verteilung.

Löschen einer Lightsail-Verteilung

Sie können IhreAmazon Lightsail-Verteilung jederzeit löschen, wenn Sie sie nicht mehr verwenden.

Löschen Ihrer Verteilung

Vervollständigen Sie das folgende Verfahren, um einen Verteilung zu löschen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen der Verteilung, die Sie löschen möchten.
4. Wählen Sie die Registerkarte Löschen auf der Verwaltungsseite Ihrer Verteilung aus.
5. Wählen Sie Verteilungen löschen, um Ihre Verteilung zu löschen.
6. Wählen Sie Yes, delete (Ja, löschen) zum Bestätigen der Löschung aus.

Ändern des Caching-Verhaltens Ihrer Lightsail-Verteilung

Mit einem Cache-Verhalten können Sie konfigurieren, was von Ihrem Ursprung durch Ihre Amazon Lightsail-Verteilung zwischengespeichert wird nicht zwischengespeichert wird. Sie können beispielsweise festlegen, dass einzelne Verzeichnisse, Dateien oder Dateitypen aus Ihrem Ursprung zwischengespeichert werden sollen. Sie können auch die HTML-Methoden und Header angeben, die an Ihren Ursprung weitergeleitet werden. In dieser Anleitung zeigen wir Ihnen, wie Sie das Caching-Verhalten Ihrer Verteilung ändern können. Weitere Informationen zu Verteilungen finden Sie unter Netzwerkverteilungen für die Bereitstellung von Inhalten.

Inhalt

- Optimal für die WordPress-Caching-Voreinstellung
- Standardverhalten
- Verzeichnis- und Dateiüberschreibungen
- Erweiterte Cache-Einstellungen
- Ändern des Cache-Verhaltens Ihrer Verteilung

Zwischenspeicherung von Voreinstellung

Eine Caching-Voreinstellung konfiguriert automatisch die Einstellungen Ihrer Verteilung für den Inhaltstyp, den Sie auf Ihrem Ursprungsserver hosten. Wählen Sie zum Beispiel die OptionOptimal für statische Inhalte, konfiguriert Ihre Verteilung automatisch mit Einstellungen, die für statische Websites am besten geeignet sind. Wenn Ihre Website auf einer WordPress-Instance gehostet wird, wählen Sie die Voreinstellung Optimal für WordPress, damit Ihre Verteilung automatisch so konfiguriert wird, dass sie mit Ihrer WordPress-Website funktioniert.

Sie können für Ihre Verteilung eine der folgenden Caching-Voreinstellungen auswählen:

- Optimal für statische Inhalte- Diese Voreinstellung konfiguriert Ihre Verteilung aufAlles cachen. Diese Voreinstellung ist ideal, wenn Sie statische Inhalte (z. B. statische HTML-Seiten) auf Ihrem Ursprungsserver hosten, oder Inhalte, die sich nicht für jeden Benutzer ändern, der Ihre Website besucht. Alle Inhalte in Ihrer Verteilung werden gecached, wenn Sie diese Voreinstellung auswählen.
- Optimal für dynamische Inhalte – Diese Voreinstellung konfiguriert Ihre Verteilung so, dass nichts außer den angegebenen Dateien gecached wird, die Sie als Cache im Abschnitt Verzeichnis- und Dateiüberschreibungen auf der Seite Eine Verteilung erstellen angeben. Weitere Informationen finden Sie unter Verzeichnis- und Dateiüberschreibungen weiter unten in diesem Leitfaden. Diese Voreinstellung ist ideal, wenn Sie dynamische Inhalte zu Ihrem Ursprungsserver hosten oder Inhalte, die sich für jeden Benutzer ändern können, der Ihre Website oder Webanwendung besucht.
- Optimal für WordPress- Diese Voreinstellung konfiguriert Ihre Verteilung aufNichts cachen mit Ausnahme der Dateien in den`wp-includes/`und`wp-content/`Verzeichnisse Ihrer WordPress-Instance. Diese Voreinstellung ist ideal, wenn Ihr Ursprungsserver eine Instance ist, die die„WordPress Certified by Bitnami“ und „Automattic-Vorlage (mit Ausnahme des Multisite-Vorlagen) verwendet. Weitere Informationen zu dieser Voreinstellung finden Sie unter Optimal für die WordPress-Caching-Voreinstellung.

> **Note**
>
> Die Voreinstellung Benutzerdefinierte Einstellungen kann nicht ausgewählt werden. Es wird automatisch für Sie ausgewählt, wenn Sie eine Voreinstellung auswählen, dann aber die Einstellungen Ihrer Verteilung manuell ändern.

Eine Caching-Voreinstellung kann nur in der Lightsail-Konsole angegeben werden. Es kann nicht angegeben werden, wenn die Lightsail-API, AWS CLI und SDKs verwendet werden.

Optimal für die WordPress-Caching-Voreinstellung

Wenn Sie eine Instance auswählen, die die WordPress Certified by Bitnami und Automattic-Vorlage als Ursprungsserver Ihrer Verteilung verwendet, fragt Lightsail, ob Sie die Option Optimal die für WordPress-Caching-Voreinstellung auf Ihre Verteilung anwenden möchten. Wenn Sie die Voreinstellung anwenden, dann wird Ihre Verteilung automatisch so konfiguriert, dass sie am besten mit Ihrer WordPress-Website funktioniert. Es gibt keine anderen Verteilungseinstellungen, die Sie anwenden müssen. Das Beste für WordPress-VoreinstellungNichts cachenmit Ausnahme der Dateien in den`wp-includes/`und`wp-content/`Verzeichnissen Ihrer WordPress-Website. Es konfiguriert auch Ihre Verteilung, um ihren Cache jeden Tag zu löschen (Cache-Lebensdauer von 1 Tag), alle HTTP-Methoden zuzulassen, nur die`Host`Kopfzeile, keine Cookies und alle Abfragezeichenfolgen weiterzuleiten.

> **Important**
>
> Sie müssen die WordPress-Konfigurationsdatei in Ihrer Instance bearbeiten, damit Ihre WordPress-Website mit Ihrer Verteilung funktioniert. Weitere Informationen finden Sie unter Konfigurieren Ihrer WordPress-Instance für die Verwendung mit Ihrer Verteilung.

Standardverhalten

Ein Standardverhaltengibt an, wie Ihre Verteilung das Inhalt-Caching verarbeitet. Das Standardverhalten Ihrer Verteilung wird automatisch für Sie festgelegt, abhängig von derCaching-Voreinstellung, die Sie auswählen. Wenn Sie ein anderes Standardverhalten auswählen, wird die Caching-Voreinstellung automatisch in Benutzerdefinierte Einstellungen geändert.

Sie können für Ihre Verteilung eine der folgenden Standardverhalten auswählen:

- Alles cachen- Durch dieses Verhalten wird Ihre Verteilung so konfiguriert, dass sie Ihre gesamte Website als statischer Inhalt zwischenspeichert und bereitgestellt wird. Diese Option ist ideal, wenn Ihr Ursprungsserver Inhalte hostet, die sich je nachdem, wer sie ansieht, nicht ändert, oder wenn Ihre Website keine Cookies, Kopfzeilen oder Abfragezeichenfolgen verwendet, um Inhalte zu personalisieren.
- Nichts cachen- Dieses Verhalten konfiguriert Ihre Verteilung so, dass nur die von Ihnen angegebenen Ursprungsdateien und Ordnerpfade gecached werden. Diese Option ist ideal, wenn Ihre Website oder Webanwendung Cookies, Kopfzeilen und Abfragezeichenfolgen verwendet, um Inhalte für einzelne Benutzer zu personalisieren. Wenn Sie diese Option auswählen, müssenSie die Verzeichnis- und Dateipfadüberschreibungen zum cachen angeben.

Verzeichnis- und Dateiüberschreibungen

EineVerzeichnis- und Dateiüberschreibungkann verwendet werden, um das von Ihnen ausgewählte Standardverhalten zu überschreiben oder eine Ausnahme hinzuzufügen. Wenn Sie beispielsweiseAlles cachen wählen, verwenden Sie eine Überschreibung, um ein Verzeichnis, eine Datei oder einen Dateityp anzugeben, den Ihre Verteilung nicht cachen soll. Wenn Sie alternativ Nichts cachen wählen, verwenden Sie eine Überschreibung, um ein Verzeichnis, eine Datei oder einen Dateityp anzugeben, den Ihre Verteilung cachen soll.

In dem Abschnitt Verzeichnis- und Dateiüberschreibungen der Seite können Sie einen Pfad zu einem Verzeichnis oder einer Datei angeben, die zwischengespeichert werden soll oder nicht zwischengespeichert werden soll. Verwenden Sie ein Sternchen-Symbol, um Platzhalterverzeichnisse (`path/to/assets/*`) und Dateitypen (`*.html`, `*jpg`, `*js`) anzugeben. Bei Verzeichnissen und Dateien muss die Groß- und Kleinschreibung beachtet werden.

Dies sind einige Beispiele, wie Sie Verzeichnis- und Dateiüberschreibungen angeben können:

- Geben Sie Folgendes an, um alle Dateien im Dokumentenstamm eines Apache-Webservers zu cachen, die auf einer Lightsail-Instance laufen.

```
var/www/html/
```

- Geben Sie die folgende Datei an, um nur die Index-Seite im Dokumentenstamm eines Apache-Webservers zu cachen.

```
var/www/html/index.html
```

- Geben Sie Folgendes an, um nur die .html-Dateien im Dokumentenstamm eines Apache-Webservers zu cachen.

```
var/www/html/*.html
```

- Geben Sie Folgendes an, um nur die .jpg,- .png- und .gif-Dateien im Images-Unterverzeichnis des Dokumentstamms eines Apache-Webservers zu cachen.

```
var/www/html/images/*.jpg
```

```
var/www/html/images/*.png
```

```
var/www/html/images/*.gif
```

  Geben Sie Folgendes an, um alle Dateien im Images-Unterverzeichnis des Dokumentstamms eines Apache-Webservers zu cachen.

```
var/www/html/images/
```

Erweiterte Cache-Einstellungen

DieErweiterte Einstellungenkönnen verwendet werden, um die Cache-Lebensdauer von Inhalten in Ihrer Verteilung, die zulässigen HTTP-Methoden, die HTTP-Kopfzeilenweiterleitung, die Cookie-Weiterleitung und die Weiterleitung von Abfragezeichenfolgen, anzugeben. Die erweiterten Einstellungen, die Sie angeben, gelten nur für das Verzeichnis und die Dateien, die Ihre Verteilung zwischenspeichert, einschließlich der Verzeichnis- und Dateiüberschreibungen, die Sie als Cache angeben.

Sie können die folgenden erweiterten Einstellungen konfigurieren:

Cache-Lebensdauer (TTL)

Steuert die Zeitspanne, in der Ihre Inhalte im Cache Ihrer Verteilung bleiben, bevor Ihre Verteilung eine weitere Anforderung an Ihren Ursprungsserver weiterleitet, um zu ermitteln, ob Ihre Inhalte aktualisiert wurden. Der Standardwert beträgt einen Tag. Eine Reduzierung der Dauer ermöglicht Ihnen, dynamische Inhalte besser bereitzustellen. Eine Erhöhung der Dauer bedeutet, dass Ihre Benutzer eine bessere Leistung erhalten, da es wahrscheinlicher ist, dass Ihre Dateien direkt vom

Edge-Standort bereitgestellt werden. Eine Erhöhung der Dauer verringert darüber hinaus die Last auf Ihrem Ursprungsserver, da Ihre Verteilung weniger häufig Inhalte abruft.

> **Note**
>
> Der angegebene Wert der Cache-Lebensdauer gilt nur, wenn Ihr Ursprungsserver keine HTTP-Kopfzeilen, wie z. B. `Cache-Control max-age`, `Cache-Control s-maxage` oder `Expires` hinzufügt.

Zulässige HTTP-Methoden

Steuert die HTTP-Methoden, die Ihre Verteilung verarbeitet und an Ihren Ursprungsserver weiterleitet. HTTP-Methoden verweisen auf die gewünschte Tätigkeit, die auf dem Ursprungsserver ausgeführt werden soll. Die GET-Methode ruft beispielsweise Daten von Ihrem Ursprungsserver ab, und die PUT-Methode fordert an, dass die abgeschlossene Einheit auf Ihrem Ursprungsserver gespeichert wird.

Sie können für Ihre Verteilung eine der folgenden Optionen für HTTP-Methoden auswählen:

- HTTP-Methoden GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE erlauben
- Erlauben der GET-, HEAD- und OPTI-Methoden
- Erlauben der GET- und HEAD-Methoden

Ihre Verteilung speichert immer Antworten auf die GET- und HEAD-Anforderungen zwischen. Ihre Verteilung speichert auch Antworten auf die OPTIONS-Anforderungen zwischen, wenn Sie diese Anforderungen erlauben. Ihre Verteilung cached keine Antworten auf Anfragen, welche die andere Methoden verwenden.

> **Important**
>
> Wenn Sie Ihre Verteilung so konfigurieren, dass alle HTTP-Methoden zulässig sind, die unterstützt werden, müssen Sie Ihre Ursprung-Instance so konfigurieren, dass alle Methoden verarbeitet werden. Wenn Sie beispielsweise Ihre Verteilung so konfigurieren, dass diese Methoden zulässig sind, weil Sie POST verwenden möchten, müssen Sie Ihren Ursprungsserver so konfigurieren, dass er DELETE-Anforderungen entsprechend erledigen kann, damit Viewer keine Ressourcen löschen können, von denen Sie nicht wünschen, dass

diese gelöscht werden. Beziehen Sie sich für weitere Informationen auf die Unterlagen für Ihre Website oder Webanwendung.

Weiterleiten der HTTP-Kopfzeile

Steuert, ob Ihre Verteilung den Inhalt, basierend auf den Werten der angegebenen Kopfzeilen, zwischenspeichert und wenn ja, welche. HTTP-Kopfzeilen enthalten Informationen über den Client-Browser, der angeforderten Seite, den Ursprung und mehr. Zum Beispiel sendet der `Accept-Language`-Header die Sprache des Kunden (beispielsweise `en-US` für Englisch), so dass der Ursprung mit Inhalten in der Sprache des Kunden antworten kann, falls diese verfügbar ist.

Sie können für Ihre Verteilung eine der folgenden HTTP-Kopfzeilen-Optionen auswählen:

- Kein Weiterleiten von Kopfzeilen
- Nur Kopfzeilen weiterleiten, die ich angebe

Wenn SieKein Weiterleiten von Kopfzeilenwählen, speichert Ihre Verteilung den Inhalt nicht basierend auf Kopfzeilenwerten zwischen. Unabhängig von der von Ihnen gewählten Option, leitet Ihre Verteilung bestimmte Kopfzeilen an Ihren Ursprungsserver weiter und führt spezifische Tätigkeiten basierend auf den von Ihnen weitergeleiteten Kopfzeilen aus.

Weiterleiten von Cookies

Steuert, ob Ihre Verteilung Cookies an Ihren Ursprungsserver weiterleitet und gegebenenfalls welche. Ein Cookie enthält einen kleinen Anteil von Daten, die an den Ursprungsserver gesendet werden, wie Informationen über die Tätigkeit eines Besuchers auf einer Webseite Ihrer Herkunft, sowie alle Informationen, die der Besucher zur Verfügung gestellt hat, wie etwa seinen Namen und Interessen.

Sie können für Ihre Verteilung eine der folgenden Cookie-Weiterleitung-Optionen auswählen:

- Keine Cookies weiterleiten
- Alle Cookies weiterleiten
- Nur Cookies weiterleiten, die ich angebe

Wenn Sie Alle weiterleiten wählen, leitet Ihre Verteilung alle Cookies weiter, unabhängig davon, wie viele Ihre Anwendung verwendet. Wenn Sie Cookies weiterleiten, die ich bestimme wählen, dann

geben Sie die Namen der Cookies ein, die Ihre Verteilung weiterleiten soll, in das angezeigte Textfeld ein. Sie können die folgenden Platzhalter angeben, wenn Sie Cookie-Namen angeben:

- * steht für 0 oder mehr Zeichen in dem Cookie-Namen
- ? steht für genau 1 Zeichen in dem Cookie-Namen

Nehmen wir beispielsweise an, dass Viewer-Anfragen für ein Objekt ein Cookie mit dem Namen `userid_member-number` beinhaltet. Dabei hat jeder Ihrer Benutzer einen eindeutigen Wert für `member-number` (`userid_123`, `userid_124`, `userid_125`). Sie möchten, dass Ihre Verteilung eine separate Version des Inhalts für jedes Mitglied zwischenspeichert. Sie könnten dies erreichen, indem Sie alle Cookies an Ihren Ursprungsserver weiterleiten. Viewer-Anfragen enthalten jedoch einige Cookies, die Sie nicht von Ihrer Verteilung zwischengespeichert haben möchten. Alternativ könnten Sie den folgenden Wert als Cookie-Namen angeben, was bewirkt, dass Ihre Verteilung alle Cookies, die mit `userid_` beginnen, an Ihren Ursprungsserver `userid_*` weiterleiten:

Weiterleiten einer Abfragezeichenfolge

Steuert, ob Ihre Verteilung Abfragezeichenfolgen an Ihren Ursprungsserver weiterleitet und gegebenenfalls welche. Eine Abfragezeichenfolge ist ein Teil einer URL, die den angegebenen Parametern Werte zuweist. Zum Beispiel beinhaltet die`https://example.com/over/there?name=ferret` URL die`name=ferret` Abfragezeichenfolge. Wenn ein Server eine Anforderung für eine solche Seite erhält, kann er ein Programm ausführen, das die`name=ferret`-Abfragezeichenfolge unverändert an das Programm weitergibt. Das Fragezeichen wird als Trennzeichen verwendet und ist nicht Teil der Abfragezeichenfolge.

Sie können festlegen, dass Ihre Verteilung keine Abfragezeichenfolgen weiterleitet oder nur die von Ihnen angegebenen. Wählen Sie diese Option aus, um Abfragezeichenfolgen nicht weiterleiten zu lassen, wenn Ihr Ursprungsserver dieselbe Version Ihres Inhalts unabhängig von den Werten der Abfragezeichenfolge-Parameter zurückgibt. Dies erhöht die Wahrscheinlichkeit, dass Ihre Verteilung eine Anfrage vom Cache bereitstellen kann, wodurch die Leistung verbessert und die Last auf Ihrem Ursprungsserver reduziert wird. Wählen Sie diese Option aus, um Abfragezeichenfolgen, die Sie angeben, weiterleiten zu lassen, wenn Ihr Ursprungsserver verschiedene Versionen Ihres Inhalts auf der Grundlage von einem oder mehreren Abfragezeichenfolge-Parametern zurückgibt.

Ändern des Cache-Verhaltens Ihrer Verteilung

Vervollständigen Sie das folgende Verfahren, um eine Verteilung zu erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.

2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen der Verteilung aus, für die Sie das Standard-Cache-Verhalten ändern möchten.
4. Wählen Sie die Registerkarte Zwischenspeichern auf der Verwaltungsseite Ihrer Verteilung aus.
5. Im Abschnitt Konfigurieren von Zwischenspeicherung der Seite wählen Sie die Zwischenspeicher-Voreinstellung für Ihre Verteilung aus. Weitere Informationen zum Caching finden Sie unter Caching-Voreinstellung.
6. Wählen Sie Ändern des Standard-Cache-Verhalten, um das Standardverhalten für Ihre Verteilung zu ändern. Wählen Sie dann ein Standardverhalten für Ihre Verteilung aus. Weitere Informationen finden Sie unter Standardverhalten.
7. (Optional) Wählen Sie Pfad hinzufügen, um ein Verzeichnis und eine Dateiüberschreibung zum Caching-Verhalten Ihrer Verteilung hinzuzufügen. Weitere Informationen finden Sie unter Verzeichnis- und Dateiüberschreibungen.
8. Wählen Sie das Stiftsymbol, das neben der erweiterten Einstellung angezeigt wird, die Sie für Ihre Verteilung bearbeiten möchten. Weitere Informationen finden Sie unter Erweiterte Cache-Einstellungen.

Wenn Sie Änderungen an der Konfiguration Ihrer Verteilung speichern, beginnt damit, die Änderungen auf alle Edge-Standorte zu übertragen. Solange die Konfiguration an einem Edge-Standort aktualisiert wird, stellt Ihre Inhalte von diesem Standort aus auf Basis der vorherigen Konfiguration bereit. Wenn die Konfiguration an einem Edge-Standort aktualisiert wurde, beginnt sofort damit, Ihre Inhalte von diesem Standort aus auf Basis der neuen Konfiguration bereitzustellen.

Ihre Änderungen werden nicht sofort auf jeden Edge-Standort übertragen. Wenn die Übertragung abgeschlossen ist, ändert sich der Status Ihrer Verteilung von InProgress zu Deployed. Während Ihre Verteilung Ihre Änderungen überträgt, können wir leider nicht feststellen, ob ein bestimmter Edge-Standort Ihre Inhalte auf Basis der vorherigen oder der neuen Konfiguration bereitstellt.

Themen

- Zurücksetzen des Caches Ihrer Lightsail-Verteilung

Zurücksetzen des Caches Ihrer Lightsail-Verteilung

Die Einstellung für die Cache-Lebensdauer (Time to Live) steuert die Zeit, die Ihre Inhalte in Ihrem Amazon Lightsail-Cache der Verteilung. Sie können den Cache in Ihrer Verteilung auch manuell

zurücksetzen, wenn Sie ihn vor dem Cache-Lebensdauerintervall löschen müssen. Nachdem Sie den Cache gelöscht haben, zieht Ihre Verteilung beim nächsten Anfordern von Inhalten die neueste Version Ihres Inhalts aus Ihrem Ursprung und speichert sie zwischendurch. In dieser Anleitung zeigen wir Ihnen, wie Sie den Cache in Ihrer Verteilung manuell zurücksetzen können. Weitere Informationen zu Verteilungen finden Sie unter Netzwerkverteilungen für die Bereitstellung von Inhalten.

Zurücksetzen des Caches Ihrer Verteilung

Vervollständigen Sie das folgende Verfahren, um eine Verteilung zu erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen der Verteilung aus, für die Sie den Cache zurücksetzen möchten.
4. Wählen Sie die Registerkarte Zwischenspeichern auf der Verwaltungsseite Ihrer Verteilung aus.
5. Scrollen Sie zum Abschnitt Cache zurücksetzen der Seite und wählen Sie Cache zurücksetzen.
6. Wählen Sie an der Bestätigungsaufforderung Ja, zurücksetzen um zu bestätigen, dass Sie den Cache Ihrer Verteilung zurücksetzen möchten. Oder wählen Sie Nein, abbrechen, um den Cache Ihrer Verteilung nicht zurückzusetzen.

Ändern des Ursprungs Ihrer Lightsail-Verteilung

In diesem Leitfaden zeigen wir Ihnen, wie Sie den Ursprung Ihrer Amazon Lightsail-Verteilung ändern, nachdem Sie sie erstellt haben. Ein Ursprungsserver ist die definitive Quelle von Inhalten für Ihre Verteilung. Wenn Sie Ihre Verteilung erstellen, wählen Sie die Lightsail-Instance, den Lightsail-Bucket oder Lightsail-Load Balancer (mit einer oder mehreren angefügten Instances), die den Inhalt Ihrer Website oder Webanwendung hostet. Weitere Informationen finden Sie unter Netzwerkverteilungen für die Bereitstellung von Inhalten.

Sie können den Ursprungsserver jederzeit ändern, nachdem Sie Ihre Verteilung erstellt haben. Wenn Sie den Ursprung ändern, beginnt Ihre Verteilung sofort mit der Replikation der Änderungen an Edge-Standorte. Solange die Verteilung weiterhin Anfragen an den vorher angegebenen Ursprung an einen bestimmten Edge-Standort noch nicht aktualisiert ist, leitet die Verteilung auf den neuen Ursprung an diesem Edge-Standort weiter.

Bei einem Wechsel des Ursprungs ist es nicht erforderlich, die Zwischenspeicher für an den Edge-Standorten mit Objekten aus dem neuen Ursprung neu mit Daten zu füllen. Solange die Benutzeranfragen in Ihrer Website oder Webanwendung nicht geändert wurden, stellt Ihre Verteilung

weiter Inhalte bereit, die sich bereits in einem Edge-Cache befinden, bis die Cache-Lebensdauer für den Inhalt abläuft.

Ursprungsprotokollrichtlinie

Die Ursprungsprotokollrichtlinie ist die Protokollrichtlinie, die Ihre Verteilung beim Abrufen von Inhalten aus Ihrem Ursprungsserver verwendet. Nachdem Sie einen Ursprungsserver für Ihre Verteilung ausgewählt haben, sollten Sie festlegen, ob Ihre Verteilung Hypertext Transfer Protocol (HTTP) oder Hypertext Transfer Protocol Secure (HTTPS) verwenden soll, wenn Inhalte aus Ihrem Ursprungsserver abgerufen werden. Wenn Ihr Ursprungsserver nicht für HTTPS konfiguriert ist, müssen Sie HTTP verwenden.

Sie können für Ihre Verteilung eine der folgenden Ursprungs-Protokollrichtlinien auswählen:

- Nur HTTP - Ihre Verteilung verwendet nur HTTP für den Zugriff auf den Ursprungsserver. Dies ist die Standardeinstellung.
- Nur HTTPS – Ihre Verteilung verwendet nur HTTPS für den Zugriff auf den Ursprungsserver.

Die Schritte zum Bearbeiten der Ursprungsprotokollrichtlinie sind im Abschnitt Eine Verteilung erstellen an späterer Stelle in diesem Leitfaden.

Ändern des Ursprung Ihrer Verteilung

Vervollständigen Sie das folgende Verfahren, um einen Verteilung zu löschen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen der Verteilung aus, für die Sie den Ursprung ändern möchten.
4. Wählen Sie die Registerkarte Details auf der Verwaltungsseite Ihrer Verteilung und scrollen Sie zum Abschnitt Wählen Sie Ihren Ursprungder Seite.

   Der Abschnitt Wählen Sie Ihren Ursprung aus der Seite zeigt den aktuellen Ursprung Ihrer Verteilung an.
5. Wählen Sie Ursprung erstellen aus.
6. Wählen Sie die AWS-Region aus, in der Ihre Ursprungsressource erstellt wurde.

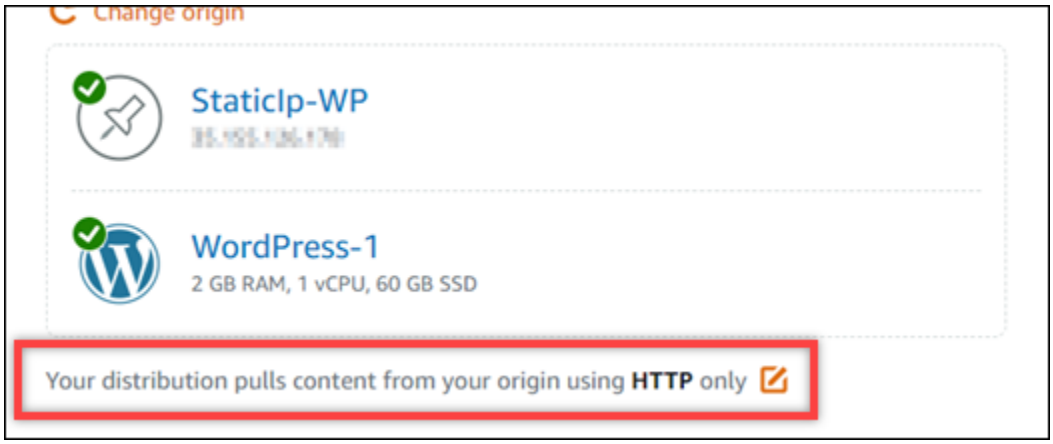
   Verteilungen sind globale Ressourcen. Sie können auf einen Ursprungsserver in jeder AWS-Region verweisen, und seinen Inhalt global verteilen.

7. Wählen Sie Ihren Ursprungsserver aus. Ein Ursprungsserver kann eine-Instance, einen Bucket oder einen Load Balancer (mit einer oder mehreren angefügten Instances) sein.
8. Wählen Sie Speichern, um Ihre Verteilung mit Ihrem neuen Ursprung zu aktualisieren.

   Nachdem Sie einen Ursprungsserver für Ihre Verteilung ausgewählt haben, sollten Sie festlegen, ob Ihre Verteilung Hypertext Transfer Protocol (HTTP) oder Hypertext Transfer Protocol Secure (HTTPS) verwenden soll, wenn Inhalte aus Ihrem Ursprungsserver abgerufen werden.
9. (Optional) Um die Ursprungsprotokollrichtlinie zu ändern, wählen Sie das Stiftsymbol, das neben der aktuellen Ursprungsprotokollrichtlinie angezeigt wird, die Ihre Verteilung verwendet. Weitere Informationen finden Sie unter Ursprungsprotokollrichtlinie.

   Diese Option ist im Abschnitt Wählen Sie Ihren Ursprungsserver der Seite unter den Ursprungs-Ressource aufgeführt, die Sie für Ihre Verteilung ausgewählt haben.

   > **Note**
   >
   > Wenn Sie wählen, einen Lightsail-Bucket als Ursprung Ihrer Verteilung zu verwenden, wird die Standardeinstellung für die Ursprungsprotokollrichtlinie auf HTTPS only (Nur HTTPS) eingestellt. Sie können die Ursprungsprotokollrichtlinie nicht ändern, wenn einen Bucket der Ursprungsserver Ihrer Verteilung ist.



10. Wählen Sie HTTP Only (Nur HTTP) oder HTTPS Only (nur HTTPS) und wählen Sie anschließend Save (Speichern) der Ursprungsprotokollrichtlinie.

Wenn Sie Änderungen an der Konfiguration Ihrer Verteilung speichern, beginnt damit, die Änderungen auf alle Edge-Standorte zu übertragen. Solange die Konfiguration an einem Edge-

Standort aktualisiert wird, stellt Ihre Inhalte von diesem Standort aus auf Basis der vorherigen Konfiguration bereit. Wenn die Konfiguration an einem Edge-Standort aktualisiert wurde, beginnt sofort damit, Ihre Inhalte von diesem Standort aus auf Basis der neuen Konfiguration bereitzustellen.

Ihre Änderungen werden nicht sofort auf jeden Edge-Standort übertragen. Wenn die Übertragung abgeschlossen ist, ändert sich der Status Ihrer Verteilung von InProgress zu Deployed. Während Ihre Verteilung Ihre Änderungen überträgt, können wir leider nicht feststellen, ob ein bestimmter Edge-Standort Ihre Inhalte auf Basis der vorherigen oder der neuen Konfiguration bereitstellt.

Änderung des Plans Ihrer Lightsail-Verteilung

Wenn Sie eine Amazon Lightsail-Verteilung erstellen, wählen Sie einen Verteilungsplan aus, der das monatliche Datenübertragungskontingent und die Kosten Ihrer Verteilung angibt. Wenn Ihre Verteilung mehr Daten überträgt als das monatliche Datenübertragungskontingent Ihres Plans, wird Ihnen eine Überschreitung in Rechnung gestellt. Weitere Informationen zu den Preisen für Überschreitung finden Sie auf der Lightsail-Preisseite.

Um eine Überschreitungsgebühr zu vermeiden, ändern Sie den aktuellen Plan Ihrer Verteilung in einen anderen Plan, der eine größere Menge an monatlichen Datenübertragungen bietet, bevor Ihre Verteilung das monatliche Kontingent überschreitet. Sie können Ihren Verteilungsplan nur einmal während jedes AWS-Abrechnungszeitraums ändern. In diesem Leitfaden zeigen wir Ihnen, wie Sie den Tarif Ihrer Verteilung ändern können.

Weitere Informationen zu Verteilungen finden Sie unter Netzwerkverteilungen für die Bereitstellung von Inhalten.

Ändern Ihres Verteilung-Tarifs

Führen Sie die folgenden Schritte aus, um den Tarif Ihrer Verteilung zu ändern.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen der Verteilung aus, für die Sie sich die aktuelle monatliche Datenübertragung anzeigen lassen möchten.
4. Wählen Sie auf der Verwaltungsseite Ihrer Verteilung die Registerkarte Details.
5. Wählen Sie im Abschnitt Datenübertragung der Seite die Option Verteilungsplan ändern.
6. Bestätigen Sie die Aufforderung mit Ja, ändern, um zu bestätigen, dass Sie den Tarif Ihrer Verteilung ändern möchten.

7. Wählen Sie in der nächsten Eingabeaufforderung den neuen Tarif für Ihre Verteilung und wählen Sie Tarif auswählen aus.
8. Wählen Sie in der nächsten Eingabeaufforderung Ja, anwenden aus, um zu bestätigen, dass Sie den neuen Tarif auf Ihre Verteilung anwenden möchten. Oder wählen Sie Nein, zurück aus, um den neuen Tarif nicht auf Ihre Verteilung anzuwenden.

Benutzerdefinierte Domains für Ihre Lightsail-Verteilung

Aktivieren benutzerdefinierter Domänen für IhreAmazon LightsailVerteilung, um Ihre registrierten Domänennamen mit Ihrer Verteilung zu verwenden. Bevor Sie benutzerdefinierte Domänen aktivieren, akzeptiert Ihre Verteilung Datenverkehr nur für die Standarddomäne, die Ihrer Verteilung zugeordnet ist, wenn Sie sie zum ersten Mal erstellen (z. B.`123456abcdef.cloudfront.net`). Wenn Sie benutzerdefinierte Domänen aktivieren, müssen Sie das LightsailSSL-/TLS-Zertifikat auswählen, das Sie für die Domänen erstellt haben, die Sie mit Ihrer Verteilung verwenden möchten. Nachdem Sie benutzerdefinierte Domänen aktiviert haben, akzeptiert Ihre Verteilung Datenverkehr für alle Domänen, die dem ausgewählten Zertifikat zugeordnet sind.

> **Important**
>
> Einer -Verteilung kann jeweils nur ein Zertifikat hinzugefügt werden. Wenn Sie benutzerdefinierte Domänen in Ihrer Verteilung deaktivieren, kann Ihre Verteilung den HTTPS-Datenverkehr für Ihre registrierte Domäne nicht mehr verarbeiten, bis Sie benutzerdefinierte Domänen erneut aktivieren.
> Die Domainnamen, die Sie beim Erstellen eines SSL-/TLS-Zertifikats für Ihre Verteilung angeben, können nicht von einer anderen Verteilung über alle Amazon Web Services (AWS)-Konten, verwendet werden, einschließlich Verteilungen auf dem Amazon-CloudFront-Service. Sie können das Zertifikat für die Domänen erstellen, aber Sie können das Zertifikat nicht mit Ihrer Verteilung verwenden.

Weitere Informationen zu Verteilungen finden Sie unter Netzwerkverteilungen für die Bereitstellung von Inhalten.

Voraussetzungen

Bevor Sie beginnen, müssen Sie eine Lightsail-Verteilung erstellen. Weitere Informationen finden Sie unter Erstellen einer Verteilung.

Außerdem sollten Sie ein SSL-/TLS-Zertifikat für Ihren Container-Service erstellt und validiert haben. Weitere Informationen finden Sie unter Erstellen von SSL-/TLS-Zertifikaten für Ihre Verteilung und Validierung von SSL-/TLS-Zertifikaten für Ihre Verteilung.

Aktivieren benutzerdefinierter Domänen für Ihre Verteilung

Vervollständigen Sie die folgenden Verfahren, um benutzerdefinierte Domänen für die Verteilung zu aktivieren.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen der Verteilung aus, für die Sie benutzerdefinierte Domänen aktivieren möchten.
4. Wählen Sie die Registerkarte Benutzerdefinierte Domänen auf der Verwaltungsseite Ihrer Verteilung aus.
5. Wählen Sie Anfügen eines Zertifikatsaus.

   Wenn Sie keine Zertifikate haben, müssen Sie zunächst ein SSL-/TLS-Zertifikat für Ihre Domains erstellen und dann validieren, bevor Sie es an Ihre Verteilung anfügen können. Weitere Informationen finden Sie unter Erstellen von SSL-/TLS-Zertifikaten für Ihre Verteilung.
6. Wählen Sie im daraufhin angezeigten Dropdown-Menü ein gültiges Zertifikat für die Domäne(n) aus, die Sie mit Ihrer Verteilung verwenden möchten.
7. Vergewissern Sie sich, dass die Zertifikatsinformationen korrekt sind, und wählen Sie dann Attach (Anfügen) aus.
8. Der Status der Verteilung wird in Updating (Wird aktualisiert) geändert. Nachdem der Status in Enabled (Aktiviert) geändert wurde, wird die Domain des Zertifikats im Abschnitt Custom domains (Benutzerdefinierte Domains) angezeigt.
9. Wählen Sie Add domain assignment (Domänenzuweisung hinzufügen) aus, um die Domäne auf Ihre Verteilung zu verweisen.
10. Vergewissern Sie sich, dass das Zertifikat und die DNS-Informationen korrekt sind, und wählen Sie dann Add assignment (Zuweisung hinzufügen). Nach einigen Augenblicken wird der Datenverkehr für die von Ihnen ausgewählte Domäne von Ihrer Verteilung akzeptiert.

Themen

- Verweisen Sie eine Domain auf Ihre Lightsail-Verteilung

- Änderung benutzerdefinierter Domains für Ihre Lightsail-Verteilung
- Deaktivieren benutzerdefinierter Domains für die Lightsail-Verteilung
- Hinzufügen der Standard-Domain einer Verteilung an einen Lightsail-Containerservice

Verweisen Sie eine Domain auf Ihre Lightsail-Verteilung

Sie müssen Ihre registrierten Domänennamen auf IhreAmazon Lightsail-Verteilung verweisen, nachdem Sie benutzerdefinierte Domänen für Ihre Verteilung aktiviert haben. Um dies zu tun, fügen Sie der DNS-Zone jeder Domäne einen Alias-Datensatzes hinzu, die in den Zertifikaten, die Sie mit Ihrem Container-Service verwenden, angegeben sind. Alle Akten, die Sie hinzufügen, sollten auf die Standarddomäne (z. B.`123456abcdef.cloudfront.net`) Ihres Container-Servicess verweisen.

In diesem Leitfaden stellen wir Ihnen das Verfahren zur Verfügung, mit dem Sie Ihre Domäne mithilfe einer Lightsail-DNS-Zone auf Ihre Verteilung verweisen können. Das Verfahren, um Ihre Domänen mithilfe eines anderen DNS-Hostinganbieters wie Domain.com oder GoDaddy auf Ihre Verteilung zu verweisen, kann ähnlich sein. Weitere Informationen über Lightsail-DNS-Zonen finden Sie unter DNS.

Weitere Informationen zu Verteilungen finden Sie unter Erstellen einer Verteilung.

Inhalt

- Schritt 1: Erfüllen der Voraussetzungen
- Schritt 2: Abrufen der Standarddomäne Ihrer Verteilung
- Schritt 3: Hinzufügen von Datensätzen zur DNS-Zone Ihrer Domäne

Schritt 1: Erfüllen der Voraussetzungen

Bevor Sie beginnen, sollten Sie benutzerdefinierte Domänen für IhreLightsail-Verteilungen aktivieren. Weitere Informationen finden Sie unter Aktivieren benutzerdefinierter Domains für Ihre Verteilung.

Schritt 2: Abrufen der Standarddomäne Ihrer Verteilung

Führen Sie das folgende Verfahren aus, um den Standard-Domänennamen Ihrer Verteilung abzurufen, den Sie beim Hinzufügen eines Alias-Datensatzes zum DNS Ihrer Domäne angeben.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.

3. Wählen Sie den Namen der Verteilung aus, für die Sie den Standarddomänennamen erhalten möchten.
4. Notieren Sie sich im Kopfbereich der Verwaltungsseite Ihrer Verteiung den Standarddomänennamen Ihrer Verteilung. Der Standarddomänenname Ihrer Verteilung ist ähnlich wie`123456abcdef.cloudfront.net`.

   Sie müssen diesen Wert als Teil eines Alias-Datensatzes im DNS Ihrer Domänen hinzufügen. Es wird empfohlen, diesen Wert in eine Textdatei zu kopieren und einzufügen, auf die Sie später verweisen können. Fahren Sie mit dem nächsten Schritt 3 fort: Fügen Sie einen Eintrag zu diesem Tutorial zum DNS-Zonenabschnitt Ihrer Domäne hinzu.

Schritt 3: Hinzufügen von Datensätzen zur DNS-Zone Ihrer Domäne

Führen Sie das folgende Verfahren aus, um Akten zur DNS-Zone Ihrer Domäne hinzuzufügen.

1. Wählen Sie auf der Lightsail-Startseite die Registerkarte Domains & DNS (Domänen und DNS).
2. Wählen Sie unter dem Abschnitt DNS-Zonen der Seite den Domänennamen aus, zu dem Sie die Akte hinzufügen möchten, der den Datenverkehr für Ihre Domäne an Ihren Verteilung weiterleitet.
3. Wählen Sie die Registerkarte DNS records (DNS-Datensätze) aus. Wählen Sie dann Add record (Datensatz hinzufügen) aus.
4. Führen Sie je nach Art der Domäne, die Sie auf die Verteilung verweisen möchten, einen der folgenden Schritte aus:

   - Wählen Sie eine Adressenakte (A), um eine Apex-Domain (z. B.`example.com`) zu Ihrer Verteilung zu verweisen.

     Wenn bereits eine A-Akte für die Spitze Ihrer Domäne in Ihrer DNS-Zone vorhanden ist, müssen Sie diese vorhandene Akte bearbeiten, anstatt eine weitere A-Akte hinzuzufügen.
   - Wählen Sie einen kanonischen Namen (CNAME), um auf eine Unterdomäne (z. B.`website.example.com`) auf Ihre Verteilung zu verweisen.
5. Wenn Sie einen A-Datesatz hinzufügen, wählen Sie im Textfeld Auflösung in den Namen Ihrer Verteilung aus. Wenn Sie eine CNAME-Akte hinzufügen, geben Sie im Textfeld Zuordnung zu den Standarddomänennamen Ihrer Verteilung ein.

> **Note**
>
> Wenn Sie der DNS-Zone einen A-Datensatz hinzufügen und den Namen Ihrer Verteilung auswählen, fügen Sie tatsächlich einen Alias-Datensatz hinzu, der sich von einem Adressen-Datensatz unterscheidet. Lightsail erleichtert Ihnen das Hinzufügen von Aliaseinträgen ohne die zusätzlichen Schritte, die normalerweise bei anderen DNS-Hosting-Anbietern erforderlich sind.

6. Wählen Sie das Symbol „Speichern“, um die Akte in Ihrer DNS-Zone zu speichern.

   Wiederholen Sie diese Schritte, um zusätzliche DNS-Akten für Domänen in Ihrem Zertifikat hinzuzufügen, das Sie mit dem Container-Service verwenden. Warten Sie einige Zeit, damit sich Änderungen über das DNS im Internet ausbreiten. Nach einigen Minuten sollten Sie sehen, ob Ihre Domäne auf Ihre Verteilung verweist. Sie sollten auch Ihre Verteilung testen. Weitere Informationen finden Sie unter Testen Ihrer Verteilung.

Änderung benutzerdefinierter Domains für Ihre Lightsail-Verteilung

Sie können die benutzerdefinierten Domänen ändern, die von IhremAmazon Lightsail-Verteilung in eine andere Domäne oder einen Satz von Domänen. Dazu müssen Sie zunächst ein neues SSL-/TLS-Zertifikat für die Domänen erstellen, die Sie mit Ihrer Verteilung verwenden möchten. Weitere Informationen finden Sie unter Erstellen von SSL-/TLS-Zertifikaten für Ihre Verteilung. Nachdem das neue Zertifikat validiert wurde, tauschen Sie das alte Zertifikat gegen das neue aus, wodurch die benutzerdefinierten Domänen für Ihre Verteilung geändert werden.

Weitere Informationen zu Verteilungen finden Sie unter Erstellen einer Verteilung.

Änderung benutzerdefinierter Domains für Ihre Verteilung

Vervollständigen Sie die folgenden Verfahren, um benutzerdefinierte Domänen für die Verteilung zu aktivieren.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen der Verteilung aus, für die Sie die benutzerdefinierten Domänen ändern möchten.

4. Wählen Sie die Registerkarte Benutzerdefinierte Domänen auf der Verwaltungsseite Ihrer Verteilung aus.
5. Trennen Sie das SSL/TLS-Zertifikat, das derzeit an die Verteilung angefügt ist.

   Der Status der Verteilung wird in In progress (In Bearbeitung) geändert.
6. Nachdem der Status der Verteilung wieder in Enabled (Aktiviert) geändert wurde, wählen Sie Attach certificate (Zertifikat anfügen) aus.
7. Wählen Sie im daraufhin angezeigten Dropdown-Menü ein gültiges Zertifikat für die Domäne(n) aus, die Sie mit Ihrer Verteilung verwenden möchten.
8. Vergewissern Sie sich, dass die Zertifikatsinformationen korrekt sind, und wählen Sie dann Attach (Anfügen) aus.
9. Fügen Sie dem DNS Ihrer Domäne eine Domänenzuweisung hinzu, um die Domäne auf Ihre Verteilung zu verweisen.

   Der Status der Verteilung wird in Updating (Wird aktualisiert) geändert. Nachdem der Status in Ready (Bereit) geändert wurde, wird die Domäne des Zertifikats im Abschnitt Custom domains (Benutzerdefinierte Domänen) angezeigt. Wählen Sie Add domain assignment (Domänenzuweisung hinzufügen) aus, um die Domäne auf Ihre Verteilung zu verweisen.
10. Wählen Add assignment (Zuweisung hinzufügen) aus. Nach einigen Augenblicken wird der Datenverkehr für die von Ihnen ausgewählte Domäne von Ihrer Verteilung akzeptiert.
11. Wählen Sie Save (Speichern).

Deaktivieren benutzerdefinierter Domains für die Lightsail-Verteilung

Deaktivieren Sie benutzerdefinierte Domänen für Ihre Amazon LightsailVerteilung, um die Verwendung Ihrer registrierten Domänennamen für Ihre Verteilung zu beenden. Nachdem Sie benutzerdefinierte Domänen deaktiviert haben, akzeptiert Ihre Verteilung nur Datenverkehr für die Standarddomäne, die Ihrer Verteilung zugeordnet wurde, als Sie sie zum ersten Mal erstellt haben (z. B.`123456abcdef.cloudfront.net`), und dem Datenverkehr für die zuvor zugeordneten benutzerdefinierten Domänen, wird ein 403-Fehler angezeigt.

Weitere Informationen zu Verteilungen finden Sie unter Netzwerkverteilungen für die Bereitstellung von Inhalten.

Deaktivieren benutzerdefinierter Domänen für die Verteilung

Vervollständigen Sie die folgenden Verfahren, um benutzerdefinierte Domänen für die Verteilung zu deaktivieren.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen der Verteilung aus, für die benutzerdefinierte Domänen deaktiviert werden sollen.
4. Wählen Sie die Registerkarte Benutzerdefinierte Domänen auf der Verwaltungsseite Ihrer Verteilung aus.

   Auf der Seite Custom domains (Benutzerdefinierte Domänen) werden die SSL-/TLS-Zertifikate angezeigt, die derzeit an Ihre Verteilung angefügt sind, falls vorhanden.
5. Wählen Sie eine der folgenden Optionen:

   1. Wählen Sie Configure distribution domains (Verteilungsdomänen konfigurieren) aus, um entweder Domänen abzuwählen, die zuvor ausgewählt wurden, oder um weitere Domänen auszuwählen, die der Verteilung zugeordnet sind.
   2. Wählen Sie Trennen, um das Zertifikat von der Verteilung zu trennen, und entfernen Sie alle zugehörigen Domains.
6. Ihre Anforderung zur Deaktivierung benutzerdefinierter Domänen wird übermittelt, und der Status Ihrer Verteilung wird zu In Bearbeitung geändert. Nach einiger Zeit ändert sich der Status Ihrer Verteilung zuAktiviert.

Nachdem Sie benutzerdefinierte Domänen deaktiviert haben, akzeptiert Ihre Verteilung nur Datenverkehr für die Standarddomäne, die Ihrer Verteilung zugeordnet wurde, als Sie sie zum ersten Mal erstellt haben (z. B.`123456abcdef.cloudfront.net`), und dem Datenverkehr für die zuvor zugeordneten benutzerdefinierten Domänen, wird ein 403-Fehler angezeigt. Sie sollten die DNS-Akten der Domänen aktualisieren, damit der Datenverkehr für diese Domänen an eine andere Ressource weitergeleitet wird.

Hinzufügen der Standard-Domain einer Verteilung an einen Lightsail-Containerservice

Sie können einen Amazon Lightsail-Containerservice als Ursprung einer Content Delivery Network (CDN)-Verteilung auswählen. Die Verteilung speichert dann die Website oder die Webanwendung, die auf Ihrem Containerservice gehostet wird und stellt sie bereit. Wenn Sie eine Lightsail-Verteilung mit Ihrem Lightsail-Containerservice verwenden, wird Lightsail automatisch der Standard Domainname Ihrer Verteilung als benutzerdefinierte Domain zu Ihrem Containerservice hinzugefügt. Auf diese Weise kann der Datenverkehr zwischen Ihrer Verteilung und Ihrem Containerservice geleitet werden. Sie müssen jedoch die in diesem Leitfaden beschriebenen Schritte ausführen, um den Standard Domainnamen Ihrer Verteilung unter den folgenden Umständen manuell zu Ihrem Containerservice hinzuzufügen:

- Wenn etwas schief geht und der Standard Domainname Ihrer Verteilung nicht automatisch zu Ihrem Containerservice hinzugefügt wird.
- Wenn Sie eine andere Verteilung als eine Lightsail-Verteilung mit Ihrem Containerservice verwenden.

Sie können den Standard-Domainnamen Ihrer Verteilung nur manuell zu Ihrem Container-Service hinzufügen, indem Sie die AWS Command Line Interface (AWS CLI) verwenden. Weitere Informationen zu Container-Services finden Sie unter Container-Services. Weitere Informationen zu Verteilungen finden Sie unter Objektspeicher.

Hinzufügen der Standard-Domain einer Verteilung an einen Containerservice

Beenden Sie das folgende Verfahren, um die Standard-Domain einer Verteilung mithilfe der AWS Command Line Interface (AWS CLI) zu einem Container-Service in Lightsail hinzuzufügen. Führen Sie dazu den Befehl `update-container-service` aus. Weitere Informationen finden Sie unter update-container-service in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail konfigurieren, bevor Sie mit diesem Vorgang fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie einen der folgenden Befehle ein, um die Standard-Domain einer Verteilung zu einem Containerservice hinzuzufügen.

> **Note**
>
> Wenn Sie Ihrem Containerservice eine benutzerdefinierte Domäne hinzugefügt haben, müssen Sie sowohl Ihre benutzerdefinierte Domäne als auch die Standarddomäne Ihrer Verteilung angeben.

Für den Containerservice ist keine benutzerdefinierte Domain konfiguriert:

```
aws lightsail update-container-service --service-name ContainerServiceName --
public-domain-names '{"_": ["DistributionDefaultDomain"]}'
```

Eine oder mehrere benutzerdefinierte Domänen sind für den Containerservice konfiguriert:

```
aws lightsail update-container-service --service-name ContainerServiceName
 --public-domain-names '{"CertificateName": ["ExistingCustomDomain"],"_":
 ["DistributionDefaultDomain"]}'
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *ContainerServiceName* – Der Name des Lightsail-Containerservices, der als Ursprung der Verteilung angegeben wurde.
- *DistributionDefaultDomain* – Die Standarddomäne der Verteilung, die den Containerservice als Ursprung verwendet. Zum Beispiel `example123.cloudfront.net`.
- *CertificateName* – Der Name des Lightsail-Zertifikats der benutzerdefinierten Domänen, die derzeit mit dem Containerservice verbunden sind, falls vorhanden. Wenn keine benutzerdefinierten Domain mit dem Containerservice verbunden sind, verwenden Sie den Befehl mit der Bezeichnung Keine benutzerdefinierte Domain ist für den Containerservice konfiguriert.
- *DistributionDefaultDomain* – Die benutzerdefinierte Domäne, die derzeit mit dem Containerservice verbunden ist.

Beispiele:

- Für den Containerservice ist keine benutzerdefinierte Domain konfiguriert:

```
aws lightsail update-container-service --service-name ContainerServiceName --
public-domain-names '{"_": ["example123.cloudfront.net"]}'
```

- Eine oder mehrere benutzerdefinierte Domänen sind für den Containerservice konfiguriert:

```
aws lightsail update-container-service --service-name ContainerServiceName
 --public-domain-names '{"example-com": ["example.com"],"_":
 ["example123.cloudfront.net"]}'
```

Anfragen- und Antwortverhalten bei Lightsail-Verteilung

In diesem Leitfaden beschreiben wir, wie sich Ihr Amazon Lightsail-Vertrieb bei der Bearbeitung und Weiterleitung von Anfragen an Ihren Absender sowie bei der Bearbeitung von Antworten von Ihrem Absender verhält. Weitere Informationen zu Verteilungen finden Sie unter Netzwerkverteilungen für die Bereitstellung von Inhalten.

Topics

Wie Ihre Verteilung Anfragen verarbeitet und an Ihren Ursprung weiterleitet

Dieser Abschnitt enthält Informationen darüber, wie Ihre Verteilung Viewer-Anfragen verarbeitet und Anfragen an Ihren Ursprung weiterleitet.

Inhalt

- Cookies
- Cross-Origin Resource Sharing (CORS)
- Verschlüsselung
- GET-Anfragen mit Anfragetext
- HTTP-Methoden
- HTTP-Anfrage-Kopfzeilen und Verteilungsverhalten
- HTTP-Version
- Maximale Länge einer Anfrage und maximale Länge einer URL
- OCSP-Stapling
- Persistente Verbindungen
- Protokolle
- Abfragezeichenfolgen
- Timeout der Ursprungsverbindung und Versuche
- Ursprungs-Reaktions-Timeout
- Gleichzeitige Anfragen für dasselbe Objekt (Datenverkehrsspitzen)
- User-Agent-Kopfzeile

Authentifizierung

Wenn Sie Ihre Verteilung für Anfragen von `DELETE`, `GET`, `HEAD`, `PATCH`, `POST`, und `PUT` so konfigurieren, dass die `Authorization`-Kopfzeile an Ihren Ursprungsserver weitergeleitet wird, können Sie Ihren Ursprungsserver so konfigurieren, dass eine Client-Authentifizierung angefordert wird.

Für `OPTIONS`-Anfragen können Sie Ihren Ursprungsserver so konfigurieren, dass eine Client-Authentifizierung nur dann angefordert wird, wenn Sie die folgenden Einstellungen verwenden:

- Konfigurieren Sie Ihre Verteilung ist so, dass die `Authorization`-Kopfzeile an den Ursprungsserver weitergeleitet wird.
- Konfigurieren Sie Ihre Verteilung so, dass die Antwort auf `OPTIONS`-Anfragen nicht zwischengespeichert wird.

Sie können Ihre Verteilung so konfigurieren, dass Anfragen an Ihren Ursprungsserver entweder über HTTP oder über HTTPS weitergeleitet werden.

Caching-Dauer

Um zu steuern, wie lange Ihre Objekte in Ihrem Vereilungs-Cache zwischengespeichert bleiben, bevor Ihre Verteilung eine weitere Anfrage an Ihren Ursprungsserver weiterleitet, können Sie:

- Ihren Ursprungsserver so konfigurieren, dass jedem Objekt ein `Cache-Control`- oder `Expires`-Header-Feld hinzugefügt wird
- Verwenden Sie den Standardwert, also 1 Tag für die Cache-Lebensdauer (TTL).

Weitere Informationen finden Sie unter Erweiterte Verteilungseinstellungen.

Client-IP-Adressen

Wenn ein Viewer eine Anfrage an Ihre Verteilung sendet und keine`X-Forwarded-For` Anfrage-Kopfzeile enthält, erhält Ihre Verteilung die IP-Adresse des Viewers der TCP-Verbindung, fügt eine `X-Forwarded-For` Kopfzeile hinzu, die eine IP-Adreese enthält und leitet die Anfrage an den Ursprungsserver weiter. Wenn z. B. Ihre Verteilung die IP-Adresse `192.0.2.2` von der TCP-Verbindung abruft, wird die folgende Kopfzeile an den Ursprungsserver weitergeleitet:

```
X-Forwarded-For: 192.0.2.2
```

Wenn ein Viewer eine Anfrage an Ihre Verteilung sendet, die eine `X-Forwarded-For`Anfrage-Kopfzeile enthält, ruft Ihre Verteilung die IP-Adresse des Viewers von der TCP-Verbindung ab, hängt diese an die `X-Forwarded-For`Kopfzeile an und leitet die Anfrage an den Ursprungsserver weiter. Wenn die Viewer-Anfrage z. B. `X-Forwarded-For: 192.0.2.4,192.0.2.3` enthält und die IP-Adresse`192.0.2.2` Ihrer Verteilung von der TCP-Verbindung abruft, wird die folgende Kopfzeile an den Ursprungsserver weitergeleitet:

```
X-Forwarded-For: 192.0.2.4,192.0.2.3,192.0.2.2
```

Manche Anwendungen wie Load Balancer, Firewalls für Webanwendungen, Reverse Proxys, Intrusion-Prevention-Systeme und API Gateway hängen die IP-Adresse des Verteilung-Edge-Servers, der die Anfrage weitergeleitet hat, an das Ende der `X-Forwarded-For`-Kopfzeile an. Wenn z. B. Ihre Verteilung `X-Forwarded-For: 192.0.2.2` in einer Anfrage beinhaltet, an die ELB weiterleitet und die IP-Adresse des Verteilung-Edge-Servers 192.0.2.199 lautet, dann enthält die Anfrage, die Ihre Instance empfängt, die folgende Kopfzeile:

```
X-Forwarded-For: 192.0.2.2,192.0.2.199
```

> **Note**
>
> Der `X-Forwarded-For`-Header kann IPv4-Adressen (z. B. 192.0.2.44) oder IPv6-Adressen (z. B. 2001:0db8:85a3:0000:0000:8a2e:0370:7334) enthalten.

Clientseitige SSL-Authentifizierung

Lightsail-Distributionen unterstützen keine Client-Authentifizierung mit clientseitigen SSL-Zertifikaten. Wenn ein Ursprungsserver ein clientseitiges Zertifikat anfordert, verwirft Ihre Verteilung die Anfrage.

Komprimierung

Lightsail-Verteilungen leiten Anfragen mit den `Accept-Encoding` Feldwerten und weiter. `"identity"` `"gzip"`

Bedingte Anforderungen

Wenn Ihre Verteilung eine Anfrage für ein Objekt erhält, das in einem Edge-Cache abgelaufen ist, wird die Anfrage an den Ursprungsserver weitergeleitet, um die neueste Version des Objekts oder eine Bestätigung vom Ursprungsserver zu erhalten, dass im Verteilung-Edge-Cache bereits die aktuelle Version enthalten ist. Als der Ursprungsserver das Objekt das letzte Mal an Ihre Verteilung gesendet hatte, war in der Regel ein `ETag`-Wert, ein `LastModified`-Wert oder beide Werte in der Antwort enthalten. In der neuen Anfrage, die Ihre Verteilung an Ihren Ursprungsserver weiterleitet, fügt Ihre Verteilung einen oder beide der folgenden Optionen hinzu:

- Einen `If-Match`- oder `If-None-Match`-Header mit dem `ETag`-Wert für die abgelaufene Version des Objekts
- Einen `If-Modified-Since`-Header mit dem `LastModified`-Wert für die abgelaufene Version des Objekts

Der Ursprungsserver verwendet diese Informationen, um zu ermitteln, ob das Objekt aktualisiert wurde bzw. ob das gesamte Objekt oder nur ein HTTP–304-Statuscode (nicht geändert) an Ihre Verteilung zurückgegeben werden muss.

Cookies

Sie können Ihre Verteilung so konfigurieren, dass Cookies an Ihren Ursprungsserver weitergeleitet werden. Weitere Informationen finden Sie unter Erweiterte Verteilungseinstellungen.

Cross-Origin Resource Sharing (CORS)

Wenn Sie möchten, dass Ihre Verteilung die Einstellungen zur ursprungsübergreifenden gemeinsamen Nutzung von Ressourcen respektiert, konfigurieren Sie Ihren Ursprungsserver so, dass die`Origin`-Kopfzeile an Ihren Ursprungsserver weitergeleitet wird.

Verschlüsselung

Sie können festlegen, dass Viewer über HTTPS eine Verbindung mit Ihrer Verteilung herstellen müssen und dass Ihre Verteilung Anforderungen mithilfe von HTTP oder HTTPS an Ihren Ursprung weiterleitet.

Ihre Verteilung leitet HTTPS-Anfragen an Ihren Ursprungsserver über die Protokolle SSLv3, TLSv1.0, TLSv1.1 und TLSv1.2 weiter. Andere Versionen von SSL und TLS werden nicht unterstützt.

GET-Anfragen mit Anfragetext

Wenn eine `GET`-Viewer-Anfrage einen Anfragetext enthält, gibt Ihre Verteilung einen HTTP-Statuscode-403 (Unzulässig) an den Viewer zurück.

HTTP-Methoden

Wenn Sie Ihre Verteilung so konfigurieren, dass alle unterstützten HTTP-Methoden verarbeitet werden, akzeptiert Ihre Verteilung die folgenden Anfragen von Viewern und leitet sie an Ihren Ursprungsserver weiter:

- `DELETE`
- `GET`
- `HEAD`
- `OPTIONS`
- `PATCH`
- `POST`
- `PUT`

Ihre Verteilung caches immer Antworten auf `GET` und `HEAD`-Anfragen. Sie können Ihre Verteilung auch so konfigurieren, dass Antworten auf `OPTIONS`-Anfragen gecached werden. Ihre Verteilung cached keine Antworten auf Anfragen, welche die andere Methoden verwenden.

Informationen zur Konfiguration Ihres Ursprungsservers für die Verarbeitung dieser Methoden finden Sie in den Unterlagen zu Ihrem Ursprungsserver.

> **Important**
>
> Wenn Sie Ihre Verteilung so konfigurieren, dass alle unterstützten HTTP-Methoden akzeptiert und an Ihren Ursprungsserver weitergeleitet werden, dann konfigurieren Sie auch Ihren Ursprungsserver so, dass alle Methoden verarbeitet werden. Wenn Sie Ihre Verteilung beispielsweise so konfigurieren, dass diese Methoden akzeptiert und weitergeleitet werden, weil Sie `POST` verwenden möchten, müssen Sie Ihren Ursprungsserver so konfigurieren, dass `DELETE`-Anfragen entsprechend verarbeitet werden, damit Viewer keine Ressourcen löschen können, die sie nicht löschen sollen. Weitere Informationen finden Sie in der Dokumentation zu Ihrem HTTP-Server.

HTTP-Anfrage-Kopfzeilen und Verteilungsverhalten

Die folgende Tabelle listet HTTP-Anfrage-Kopfzeilen auf, die Sie an Ihren Ursprungsserver weiterleiten können (mit Ausnahmen, auf die hingewiesen wird). Für jede Kopfzeile umfasst die Tabelle Informationen über Folgendes:

- Unterstützt – Ob Sie Ihre Verteilung so konfigurieren können, dass Objekte auf Basis der Kopfzeilen-Werte für diese Kopfzeile im Cache gespeichert werden.

  Sie können Ihre Verteilung so konfigurieren, dass Objekte auf der Grundlage von Werten in den `Date` und `User-Agent`-Kopfzeilen gecached werden; dies wird jedoch nicht empfohlen. Diese Kopfzeilen können eine Vielzahl möglicher Werte enthalten; das Caching auf Basis dieser Werte würde dazu führen, dass wesentlich mehr Anfragen von Ihrer Verteilung an Ihren Ursprungsserver weitergeleitet werden.
- Verhalten, wenn Sie nicht konfigurieren – Das Verhalten Ihrer Verteilung, wenn Sie diese nicht konfigurieren, um die Kopfzeile an Ihren Ursprungsserver weiterzuleiten, welches Ihre Verteilung dazu bringt, Ihre Objekte auf Basis der Kopfzeilen-Werten im Cache zu speichern.

- Kopfzeile – Anderweitig definierte Kopfzeilen

  Unterstützt – Ja

Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `Accept`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung entfernt die Kopfzeile.

- Kopfzeile – `Accept-Charset`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung entfernt die Kopfzeile.

- Kopfzeile – `Accept-Encoding`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Wenn der Wert `gzip` enthält, leitet Ihre Verteilung `Accept-Encoding: gzip` an Ihren Ursprungsserver weiter. Wenn der Wert `gzip` nicht enthält, entfernt Ihre Verteilung das Kopfzeilen-Feld `Accept-Encoding`, bevor die Anfrage an Ihren Ursprungsserver weitergeleitet wird.

- Kopfzeile – `Accept-Language`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung entfernt die Kopfzeile.

- Kopfzeile – `Authorization`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert:

  - `GET`- und `HEAD`-Anfragen – Ihre Verteilung entfernt das `Authorization`-Header-Feld, bevor die Anfrage an Ihren Ursprung weitergeleitet wird.
  - `OPTIONS`-Anforderungen – Ihre Verteilung entfernt das `Authorization`-Header-Feld, bevor die Anfrage an Ihren Ursprung weitergeleitet wird, wenn Sie Ihre Verteilung so konfigurieren, dass Antworten auf `OPTIONS`-Anfragen im Cache gespeichert werden.

Ihre Verteilung leitet das `Authorization` Kopfzeilen-Feld an Ihren Ursprungsserver weiter, wenn Sie Ihre Verteilung nicht so konfigurieren, dass Antworten auf OPTIONS-Anfragen im Cache gespeichert werden.

- `DELETE`-, `PATCH`-, `POST`- und `PUT`-Anforderungen – Ihre Verteilung entfernt das Kopfzeilen-Feld nicht, bevor die Anfrage an Ihren Ursprung weitergeleitet wird.

- Kopfzeile – `Cache-Control`

  Unterstützt - Nein

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `CloudFront-Forwarded-Proto`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung fügt die Kopfzeile nicht hinzu, bevor die Anfrage an den Ursprungsserver weitergeleitet wird.

- Kopfzeile – `CloudFront-Is-Desktop-Viewer`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung fügt die Kopfzeile nicht hinzu, bevor die Anfrage an den Ursprungsserver weitergeleitet wird.

- Kopfzeile – `CloudFront-Is-Mobile-Viewer`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung fügt die Kopfzeile nicht hinzu, bevor die Anfrage an den Ursprungsserver weitergeleitet wird.

- Kopfzeile – `CloudFront-Is-Tablet-Viewer`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung fügt die Kopfzeile nicht hinzu, bevor die Anfrage an den Ursprungsserver weitergeleitet wird.

- Kopfzeile – `CloudFront-Viewer-Country`

  Unterstützt – Ja

Verhalten, wenn nicht konfiguriert – Ihre Verteilung fügt die Kopfzeile nicht hinzu, bevor die Anfrage an den Ursprungsserver weitergeleitet wird.

- Kopfzeile – `Connection`

  Unterstützt – Nein

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung ersetzt diese Kopfzeile durch`Connection: Keep-Alive` bevor die Anfrage an Ihren Ursprungsserver weitergeleitet wird.

- Kopfzeile – `Content-Length`

  Unterstützt - Nein

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `Content-MD5`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `Content-Type`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `Cookie`

  Unterstützt – Nein

  Verhalten, wenn nicht konfiguriert – Wenn Sie Ihre Verteilung so konfigurieren, dass Cookies weitergeleitet werden, wird die `Cookie`-Kopfzeile an Ihren Ursprungsserver weitergeleitet. Wenn Sie das nicht tun, entfernt Ihre Verteilung das `Cookie`Kopfzeilen-Feld.

- Kopfzeile – `Date`

  Unterstützt – Ja, wird aber nicht empfohlen

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `Expect`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung entfernt die Kopfzeile.

- Kopfzeile – `From`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `Host`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung stellt den Wert auf den Domänennamen des Ursprungsservers ein, der dem angeforderten Objekt zugeordnet ist.

- Kopfzeile – `If-Match`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `If-Modified-Since`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `If-None-Match`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `If-Range`

  Unterstützt – Ja

Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `If-Unmodified-Since`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `Max-Forwards`

  Unterstützt - Nein

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `Origin`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `Pragma`

  Unterstützt - Nein

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `Proxy-Authenticate`

  Unterstützt – Nein

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung entfernt die Kopfzeile.

- Kopfzeile – `Proxy-Authorization`

  Unterstützt – Nein

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung entfernt die Kopfzeile.

- Kopfzeile – `Proxy-Connection`

  Unterstützt – Nein

Verhalten, wenn nicht konfiguriert – Ihre Verteilung entfernt die Kopfzeile.

- Kopfzeile – `Range`

  Unterstützt- Ja, standardmäßig

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `Referer`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung entfernt die Kopfzeile.

- Kopfzeile – `Request-Range`

  Unterstützt – Nein

  Verhalten, wenn nicht konfiguriert – >Ihre Verteilung leitet die Kopfzeile an Ihren Ursprungsserver weiter.

- Kopfzeile – `TE`

  Unterstützt – Nein

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung entfernt die Kopfzeile.

- Kopfzeile – `Trailer`

  Unterstützt – Nein

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung entfernt die Kopfzeile.

- Kopfzeile – `Transfer-Encoding`

  Unterstützt - Nein

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `Upgrade`

  Unterstützt — Nein (außer für Verbindungen) WebSocket

Verhalten, wenn nicht konfiguriert — Ihre Distribution entfernt den Header, sofern Sie keine WebSocket Verbindung hergestellt haben.

- Kopfzeile – `User-Agent`

  Unterstützt – Ja, wird aber nicht empfohlen

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung ersetzt den Wert dieses Kopfzeilen-Felds durch`Amazon CloudFront`.

- Kopfzeile – `Via`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `Warning`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `X-Amz-Cf-Id`

  Unterstützt – Nein

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung fügt die Kopfzeile der Viewer-Anfrage hinzu, bevor die Anfrage an Ihren Ursprungsserver weitergeleitet wird. Der Header-Wert enthält eine verschlüsselte Zeichenfolge, die die Anfrage eindeutig bezeichnet.

- Kopfzeile – `X-Edge-*`

  Unterstützt – Nein

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung entfernt alle `X-Edge-*`-Kopfzeilen.

- Kopfzeile – `X-Forwarded-For`

  Unterstützt – Ja

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung leitet die Kopfzeilen an Ihren Ursprungsserver weiter.

- Kopfzeile – `X-Forwarded-Proto`

  Unterstützt – Nein

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung entfernt die Kopfzeile.
- Kopfzeile – `X-Real-IP`

  Unterstützt – Nein

  Verhalten, wenn nicht konfiguriert – Ihre Verteilung entfernt die Kopfzeile.

HTTP-Version

Ihre Verteilung leitet Anfragen an Ihren Ursprungsserver über HTTP/1.1 weiter.

Maximale Länge einer Anfrage und maximale Länge einer URL

Die maximale Länge einer Anfrage – einschließlich des Pfads, der Abfragezeichenfolge (falls vorhanden) und der Header – beträgt 20 480 Byte.

Die Verteilung erstellt eine URL auf Grundlage der Anfrage. Die maximale Länge dieser URL beträgt 8 192 Byte.

Wenn eine Anfrage oder eine URL diese Höchstwerte überschreitet, gibt Ihre Verteilung einen HTTP-Statuscode-413, Request Entity Too Large, an den Viewer zurück; anschließend wird die TCP-Verbindung mit dem Viewer beendet.

OCSP-Stapling

Wenn ein Viewer eine HTTPS-Anfrage für ein Objekt sendet, muss entweder Ihre Verteilung oder der Viewer bei der Zertifizierungsstelle (CA) bestätigen, dass das SSL-Zertifikat für die Domäne nicht widerrufen wurde. OCSP-Stapling beschleunigt die Validierung des Zertifikats, indem Ihrer Verteilung gestattet wird, das Zertifikat zu validieren und die Antwort von der CA im Cache zu speichern, sodass der Client das Zertifikat nicht direkt bei der CA validieren muss.

Die Leistungssteigerung durch OCSP-Stapling ist deutlicher spürbar, wenn Ihre Verteilung viele HTTPS-Anfragen für Objekte in derselben Domäne erhält. Jeder Server an einem Verteilung-Edge-Standort muss eine separate Validierungsanfrage senden. Wenn Ihre Verteilung viele HTTPS-Anfragen für dieselbe Domäne erhält, hat jeder Server an dem Edge-Standort nach kurzer Zeit

eine Antwort von der CA vorliegen, die er an ein Paket im SSL-Handshake „stapeln“ kann; wenn der Viewer mit der Gültigkeit des Zertifikats zufrieden ist, kann Ihre Verteilung das angeforderte Objekt bereitstellen. Wenn Ihre Verteilung nicht viel Datenverkehr an einem Edge-Standort generiert, werden neue Anfragen mit einer höheren Wahrscheinlichkeit an einen Server weitergeleitet, der das Zertifikat noch nicht bei der CA validiert hat. In diesem Fall führt der Viewer den Validierungsschritt selbst aus und der -Server überträgt das Objekt. Dieser Verteilungsserver sendet außerdem eine Validierungsanfrage an die CA; wenn er das nächste Mal eine Anfrage mit demselben Domänenamen erhält, liegt bereits eine Validierungsantwort von der CA vor.

Persistente Verbindungen

Wenn Ihre Verteilung eine Antwort von Ihrem Ursprungsserver erhält, wird dieser versuchen, die Verbindung mehrere Sekunden lang aufrechtzuerhalten – für den Fall, dass während dieses Zeitraums eine weitere Anfrage eingeht. Durch eine persistente Verbindung wird Zeit gespart, die erforderlich ist, um die TCP-Verbindung erneut herzustellen und einen weiteren TLS-Handshake für nachfolgende Anforderungen durchzuführen.

Protokolle

Ihre Distribution leitet HTTP- oder HTTPS-Anfragen an den Ursprungsserver weiter, basierend auf dem Wert des Origin-Protokollrichtlinienfeldes in der Lightsail-Konsole. In der Lightsail-Konsole sind die Optionen nur HTTP und nur HTTPS verfügbar.

Wenn Sie Nur HTTP oder Nur HTTPS angeben, leitet Ihre Verteilung Anfragen an Ihren Ursprungsserver weiter, unabhängig vom Protokoll der Viewer-Anfrage.

> **Important**
>
> Wenn Ihre Verteilung eine Anfrage an Ihren Ursprungsserver über das HTTPS-Protokoll weiterleitet und der Ursprungsserver ein ungültiges oder selbstsigniertes Zertifikat zurückgibt, verwirft Ihre Verteilung die TCP-Verbindung.

Abfragezeichenfolgen

Sie können konfigurieren, ob Ihre Verteilung Abfragezeichenfolgeparameter an Ihren Ursprung weiterleitet.

Timeout der Ursprungsverbindung und Versuche

Ihre Verteilung wartet standardmäßig bis zu 30 Sekunden (3 Versuche à 10 Sekunden), bevor eine Fehlermeldung an den Viewer zurückgegeben wird.

Ursprungs-Reaktions-Timeout

Das Ursprungs-Reaktions-Timeout, das auch als Ursprungs-Lese-Timeout oder Ursprungs-Anforderungs-Timeout bezeichnet wird, gilt für Folgendes:

- Die Zeit in Sekunden, die Ihre Verteilung nach der Weiterleitung einer Anforderung an den Ursprungsserver auf eine Antwort wartet.
- Die Zeit in Sekunden, die Ihre Verteilung nach dem Erhalt eines Antwortpakets vom Ursprungsserver und vor dem Empfang des nächsten Pakets wartet.

Das Verhalten Ihrer Verteilung ist von der HTTP-Methode der Viewer-Anfrage abhängig:

- `GET`- und `HEAD`-Anfragen – Wenn der Ursprung nicht innerhalb der Dauer des Reaktions-Timeouts reagiert oder nicht mehr reagiert, verwirft Ihre Verteilung die Verbindung. Wenn die angegebene Anzahl von Verbindungsversuchen zum Ursprung mehr als 1 beträgt, versucht Ihre Verteilung erneut, eine vollständige Antwort zu erhalten. Ihre Verteilung versucht dies bis zu 3 Mal, wie im Wert der Einstellung Verbindungsversuche zum Ursprungsserver festgelegt. Wenn der Ursprung beim letzten Versuch keine Antwort sendet, unternimmt Ihre Verteilung erst dann einen weiteren Versuch, wenn die nächste Anfrage für Inhalte auf demselben Ursprung empfangen wird.
- `DELETE`-, `OPTIONS`-, `PATCH`-, `PUT`- und `POST`-Anfragen Wenn der Ursprung nicht innerhalb von 30 Sekunden reagiert, verwirft Ihre Verteilung die Verbindung und versucht nicht, den Ursprung erneut zu kontaktieren. Der Client kann die Anfrage erneut senden, falls erforderlich.

Gleichzeitige Anfragen für dasselbe Objekt (Datenverkehrsspitzen)

Wenn ein Verteilung-Edge-Standort eine Anfrage für ein Objekt erhält und sich das Objekt zu dem Zeitpunkt entweder nicht im Cache befindet oder bereits abgelaufen ist, sendet Ihre Verteilung die Anfrage sofort an Ihren Ursprungsserver. Wenn eine Datenverkehrsspitze vorliegt – also weitere Anfragen für dasselbe Objekt am Edge-Standort ankommen, bevor Ihr Ursprung auf die erste Anfrage geantwortet hat – legt Ihre Verteilung eine kurze Pause ein, bevor die weiteren Anfragen für das Objekt an Ihren Ursprung weitergeleitet werden. In der Regel erreicht die Antwort auf die

erste Anfrage den Verteilung-Edge-Standort vor der Antwort auf die nachfolgenden Anfragen. Diese kurze Pause trägt dazu bei, unnötige Arbeitslasten auf Ihrem Ursprungsserver zu vermeiden. Wenn die weiteren Anfragen nicht identisch sind, da Sie Ihre Verteilung z. B. so konfiguriert haben, dass Objekte auf Basis der Anfrage-Kopfzeilen oder Cookies im Cache gespeichert werden, leitet Ihre Verteilung alle eindeutigen Anfragen an Ihren Ursprungsserver weiter.

Benutzer-Agent-Kopfzeile

Wenn Sie möchten, dass Ihre Verteilung verschiedene Versionen Ihrer Objekte basierend auf dem Gerät zwischenspeichert, das ein Benutzer zum Anzeigen Ihrer Inhalte verwendet, empfehlen wir, Ihre Verteilung so zu konfigurieren, dass mindestens einer der folgenden Kopfzeilen an Ihren Ursprungsserver weitergeleitet wird:

- `CloudFront-Is-Desktop-Viewer`
- `CloudFront-Is-Mobile-Viewer`
- `CloudFront-Is-SmartTV-Viewer`
- `CloudFront-Is-Tablet-Viewer`

Auf der Grundlage des Werts der `User-Agent`-Kopfzeile stellt Ihre Verteilung den Wert dieser Kopfzeilen auf `true` oder `false` ein, bevor die Anfrage an Ihren Ursprungsserver weitergeleitet wird. Wenn ein Gerät in mehr als eine Kategorie fällt, können mehrere Werte sei `true`. Beispielsweise stellt Ihre Verteilung bei einigen Tablet-Geräten möglicherweise beide `CloudFront-Is-Mobile-Viewer` und `CloudFront-Is-Tablet-Viewer` auf `true` ein.

Sie können Ihre Verteilung so konfigurieren, dass Objekte auf der Grundlage von Werten in der `User-Agent`-Kopfzeile gecached werden; dies wird jedoch nicht empfohlen. Die `User-Agent`-Kopfzeile kann eine Vielzahl möglicher Werte enthalten; das Caching auf Basis dieser Werte würde dazu führen, dass wesentlich mehr Anfragen von Ihrer Verteilung an Ihren Ursprungsserver weitergeleitet werden.

Wenn Sie Ihre Verteilung nicht so konfigurieren, dass Objekte auf Basis der Werte in der `User-Agent`-Kopfzeile im Cache gespeichert werden, wird in Ihrer Verteilung eine `User-Agent`-Kopfzeile mit dem folgenden Wert hinzugefügt, bevor eine Anfrage an Ihren Ursprungsserver weitergeleitet wird:

```
User-Agent = Amazon CloudFront
```

Ihre Verteilung fügt diese Kopfzeile unabhängig davon hinzu, ob die Anfrage vom Viewer eine `User-Agent`-Kopfzeile enthält. Wenn in der Anfrage vom Viewer eine `User-Agent`-Kopfzeile enthalten ist, wird dieser von Ihrer Verteilung entfernt.

Wie Ihre Verteilung Antworten von Ihrem Ursprungsserver verarbeitet

Dieser Abschnitt enthält Informationen darüber, wie Ihre Verteilung Antworten von Ihrem Ursprung verarbeitet.

Inhalt

100 Continue-Antworten

Ihr Ursprungsserver kann nicht mehr als eine 100 Continue-Antwort an Ihre Verteilung senden. Nach der ersten 100 Continue-Antwort erwartet Ihre Verteilung eine 200-OK-HTTP-Antwort. Wenn Ihr Ursprungsserver nach der ersten eine weitere 100 Continue-Antwort sendet, gibt Ihre Verteilung einen Fehler zurück.

Caching

- Stellen Sie sicher, dass Ihr Ursprungsserver in den Kopfzeilen-Feldern `Date` und `Last-Modified` gültig und korrekte Werte einsetzt.

- Wenn in den Anfragen von Viewern das Anfrage-Header-Feld `If-Match` oder `If-None-Match` enthalten ist, fügen Sie ein `ETag`-Antwort-Header-Feld ein. Wenn Sie keinen `ETag`-Wert angeben, ignoriert Ihre Verteilung die nachfolgenden `If-Match` oder `If-None-Match`-Kopfzeilen.
- In der Regel respektiert Ihre Verteilung eine `Cache-Control: no-cache`-Kopfzeile in der Antwort des Ursprungsservers. Eine Ausnahme von dieser Regel finden Sie unterGleichzeitige Anfragen für dasselbe Objekt (Verkehrsspitzen).

Abgebrochene Anfragen

Wenn sich ein Objekt nicht im Edge-Cache befindet und der Viewer die Sitzung beendet (z.B. einen Browser schließt), nachdem das Objekt von Ihrem Ursprungsserver an Ihre Verteilung gesendet wurde aber noch bevor das angeforderte Objekt übertragen werden konnte, wird das Objekt von Ihrer Verteilung nicht an dem Edge-Standort zwischengespeichert.

Inhaltsvereinbarung

Wenn Ihr Ursprungsserver in der Antwort `Vary:*` zurückgibt und der Wert von Minimum TTL für das entsprechende Cache-Verhalten 0 ist, wird das Objekt von Ihrer Verteilung im Cache gespeichert. Jede nachfolgende Anfrage für das Objekt wird aber dennoch an den Ursprungsserver weitergeleitet, um bestätigen, dass die neueste Version des Objekts im Cache enthalten ist. Ihre Verteilung schließt keine bedingten Kopfzeilen wie z. B. `If-None-Match` oder `If-Modified-Since` ein. Dies hat zur Folge, dass Ihr Ursprung das Objekt als Antwort bei jeder Anfrage an Ihre Verteilung zurückgibt.

Wenn Ihr Ursprung `Vary:*` in der Antwort zurückgegeben wird und wenn der Wert von Minimum TTL für das entsprechende Cache-Verhalten ein anderer Wert ist, CloudFront verarbeitet der `Vary` Header wie in HTTP-Antwort-Headern beschrieben, die Ihre Distribution entfernt oder ersetzt.

Cookies

Wenn Sie Cookies für ein Cache-Verhalten aktivieren und der Ursprungsserver die Cookies zusammen mit einem Objekt zurückgibt, speichert Ihre Verteilung das Objekt und die Cookies im Cache. Beachten Sie, dass dies die Cache-Fähigkeit für ein Objekt reduziert.

Verworfene TCP-Verbindungen

Wenn die TCP-Verbindung zwischen Ihrer Verteilung und Ihrem Ursprungsserver verworfen wird, während Ihr Ursprungsserver ein Objekt an Ihre Verteilung sendet, ist das Verhalten Ihrer Verteilung davon abhängig, ob in der Antwort Ihres Ursprungsservers eine `Content-Length`-Kopfzeile enthalten ist:

- Inhaltslängen-Header – Ihre Verteilung gibt das Objekt an den Viewer zurück, wenn das Objekt von Ihrem Ursprung empfangen wird. Wenn der Wert der `Content-Length`-Kopfzeile jedoch nicht der tatsächlichen Größe des Objekts entspricht, speichert Ihre Verteilung das Objekt nicht im Cache.
- Übertragungsverschlüsselung: Gestückelt – Ihre Verteilung gibt das Objekt an den Viewer zurück, wenn das Objekt von Ihrem Ursprung empfangen wird. Wenn die gestückelte Antwort jedoch nicht vollständig ist, speichert Ihre Verteilung das Objekt nicht im Cache.
- Kein-Inhalt–Länge-Header – Ihre Verteilung gibt das Objekt an den Viewer zurück und speichert es im Cache, aber das Objekt ist möglicherweise nicht vollständig. Ohne eine `Content-Length`-Kopfzeile kann Ihre Verteilung nicht bestimmen, ob die TCP-Verbindung versehentlich oder absichtlich verworfen wurde.

Wir empfehlen, dass Sie Ihren HTTP-Server so konfigurieren, dass eine `Content-Length`-Kopfzeile hinzugefügt wird. So können Sie vermeiden, dass Ihre Verteilung unvollständige Objekte im Cache speichert.

HTTP-Antwort-Kopfzeilen, die von Ihrer Verteilung entfernt oder ersetzt werden

Ihre Verteilung entfernt oder aktualisiert die folgenden Kopfzeilen-Felder, bevor die Antworten von Ihrem Ursprungsserver an den Viewer weitergeleitet werden:

- `Set-Cookie` – Wenn Sie Ihre Verteilung so konfigurieren, dass Cookies weitergeleitet werden, wird das `Set-Cookie`-Header-Feld an die Clients weitergeleitet.
- `Trailer`
- `Transfer-Encoding` – Wenn Ihr Ursprung dieses Header-Feld zurückgibt, setzt Ihre Verteilung den Wert auf `chunked`, bevor die Antwort an den Viewer zurückgegeben wird.
- `Upgrade`
- `Vary` – Beachten Sie Folgendes:
  - Wenn Sie Ihre Verteilung so konfigurieren, dass alle gerätespezifischen Kopfzeilen an Ihren Ursprungsserver (`CloudFront-Is-Desktop-Viewer`, `CloudFront-Is-Mobile-Viewer`, `CloudFront-Is-SmartTV-Viewer`, `CloudFront-Is-Tablet-Viewer`) weitergeleitet werden, und Sie Ihren Ursprungsserver so konfigurieren, dass `Vary:User-Agent` an Ihre Verteilung zurückgegeben wird, dann gibt Ihre Verteilung `Vary:User-Agent` an den Viewer zurück.
  - Wenn Sie Ihren Ursprungsserver so konfigurieren, dass entweder `Accept-Encoding` oder `Cookie` in der `Vary`-Kopfzeile enthalten ist, dann fügt Ihre Verteilung diese Werte in die Antwort an den Viewer ein.

- Wenn Sie Ihre Distribution so konfigurieren, dass sie eine Zulassungsliste mit Headern an Ihren Ursprung weiterleitet, und wenn Sie Ihren Ursprung so konfigurieren, dass die Header-Namen Ihrer Distribution in der `Vary` Kopfzeile zurückgegeben werden (zum Beispiel`Vary:Accept-Charset,Accept-Language`), gibt Ihre Distribution den `Vary` Header mit diesen Werten an den Viewer zurück.
- Informationen darüber, wie Ihre Verteilung einen Wert von`*` in der `Vary`-Kopfzeile verarbeitet, siehe Inhaltsverhandlung.
- Wenn Sie Ihren Ursprungsserver so konfigurieren, dass andere Werte in der `Vary` Kopfzeile enthalten sind, dann entfernt Ihre Verteilung diese Werte, bevor die Antwort an den Viewer zurückgegeben wird.

- `Via` – Ihre Verteilung legt bei der Antwort an den Viewer den Wert wie folgt fest:

  `Via: http-version alphanumeric-string.cloudfront.net (CloudFront)`

  Beispiel: Wenn der Client eine Anfrage über HTTP/1.1 stellt, sieht der Wert in etwa wie folgt aus:

  ```
  Via: 1.1 1026589cc7887e7a0dc7827b4example.cloudfront.net (CloudFront)
  ```

Maximale Dateigröße

Die maximale Größe des Inhalts einer Antwort, die Ihre Verteilung an den Viewer zurückgibt, beträgt 20 GB. Dazu gehören auch Antworten für aufgeteilte Übertragungen, in denen kein Wert für die `Content-Length`-Kopfzeile angegeben wurde.

Ursprung nicht verfügbar

Wenn Ihr Ursprungsserver nicht verfügbar ist und Ihre Verteilung eine Anfrage für ein Objekt erhält, das zwar im Edge-Cache vorhanden aber abgelaufen ist (z. B. da der in der `Cache-Control max-age`-Richtlinie angegebene Zeitraum verstrichen ist), stellt Ihre Verteilung entweder die abgelaufene Version des Objekts oder eine benutzerdefinierte Fehlerseite bereit.

In manchen Fällen wird ein selten angefordertes Objekt entfernt und ist nicht mehr im Edge-Cache verfügbar. Ihre Verteilung kann ein Objekt, das bereinigt wurde, nicht bereitstellen.

Umleitungen

Wenn Sie den Speicherort eines Objekts auf dem Ursprungsserver ändern, können Sie Ihren Webserver so konfigurieren, dass Anfragen an den neuen Speicherort umgeleitet werden. Wenn ein Viewer nach der Einrichtung der Umleitung zum ersten Mal eine Objektanforderung sendet, leitet Ihre

Verteilung die Anfrage an den Ursprungsserver weiter und dieser antwortet mit einer Umleitung (z. B. `302 Moved Temporarily`). Ihre Verteilung speichert die Umleitung im Cache und gibt sie an den Viewer zurück. Ihre Verteilung folgt der Umleitung nicht.

Sie können Ihren Webserver so konfigurieren, dass Anfragen an einen der folgenden Speicherorte umgeleitet werden:

- Die neue URL des Objekts auf dem Ursprungsserver. Wenn der Viewer der Umleitung auf die neue URL folgt, umgeht der Viewer Ihre Verteilung und geht direkt an den Ursprungsserver. Daher empfehlen wir, dass Sie Anfragen nicht auf die neue URL des Objekts auf dem Ursprungsserver weiterleiten.
- Die neue Verteilung-URL für das Objekt. Wenn der Viewer die Anfrage mit der neuen Verteilung-URL sendet, ruft Ihre Verteilung das Objekt von dem neuen Speicherort auf Ihrem Ursprungsserver ab, speichert es am Edge-Standort zwischen und gibt das Objekt an den Viewert zurück. Nachfolgende Anfragen für das Objekt werden von dem Edge-Standort bedient. Dadurch werden Latenzzeiten und Arbeitslasten vermieden, die bei Viewer-Anforderungen für das Objekt an den Ursprungsserver entstehen. Allerdings werden bei jeder neuen Anfrage für das Objekt Gebühren für zwei Anfragen an Ihre Verteilung berechnet.

Übertragungsverschlüsselungen

Lightsail-Distributionen unterstützen nur den `chunked` Wert des Headers. `Transfer-Encoding` Wenn Ihr Ursprungsserver `Transfer-Encoding: chunked` zurückgibt, sendet Ihre Verteilung das Objekt an den Client, sobald es am Edge-Standort empfangen wird, und speichert das Objekt im aufgeteilten Format für nachfolgende Anfragen zwischen.

Wenn der Viewer eine `Range GET`-Anfrage stellt und der Ursprungsserver `Transfer-Encoding: chunked` zurückgibt, gibt Ihre Verteilung das gesamte Objekt anstelle des angefragten Bereichs an den Viewer zurück.

Wir empfehlen, dass Sie die Abschnittscodierung verwenden, wenn die Länge des Inhalts Ihrer Antwort nicht im Voraus ermittelt werden kann. Weitere Informationen finden Sie unterVerworfene TCP-Verbindungen.

Testen Ihrer Lightsail-Verteilung

In diesem Leitfaden zeigen wir Ihnen, wie Sie testen können, ob Ihre Amazon Lightsail-Verteilung Caching und Bereitstellung von Inhalten aus Ihrem Ursprung vornimmt. Sie sollten diesen Test

durchführen, nachdem Sie Ihren registrierten Domainnamen zu Ihrer Verteilung hinzugefügt haben. Weitere Informationen zu Verteilungen finden Sie unter Netzwerkverteilungen für die Bereitstellung von Inhalten.

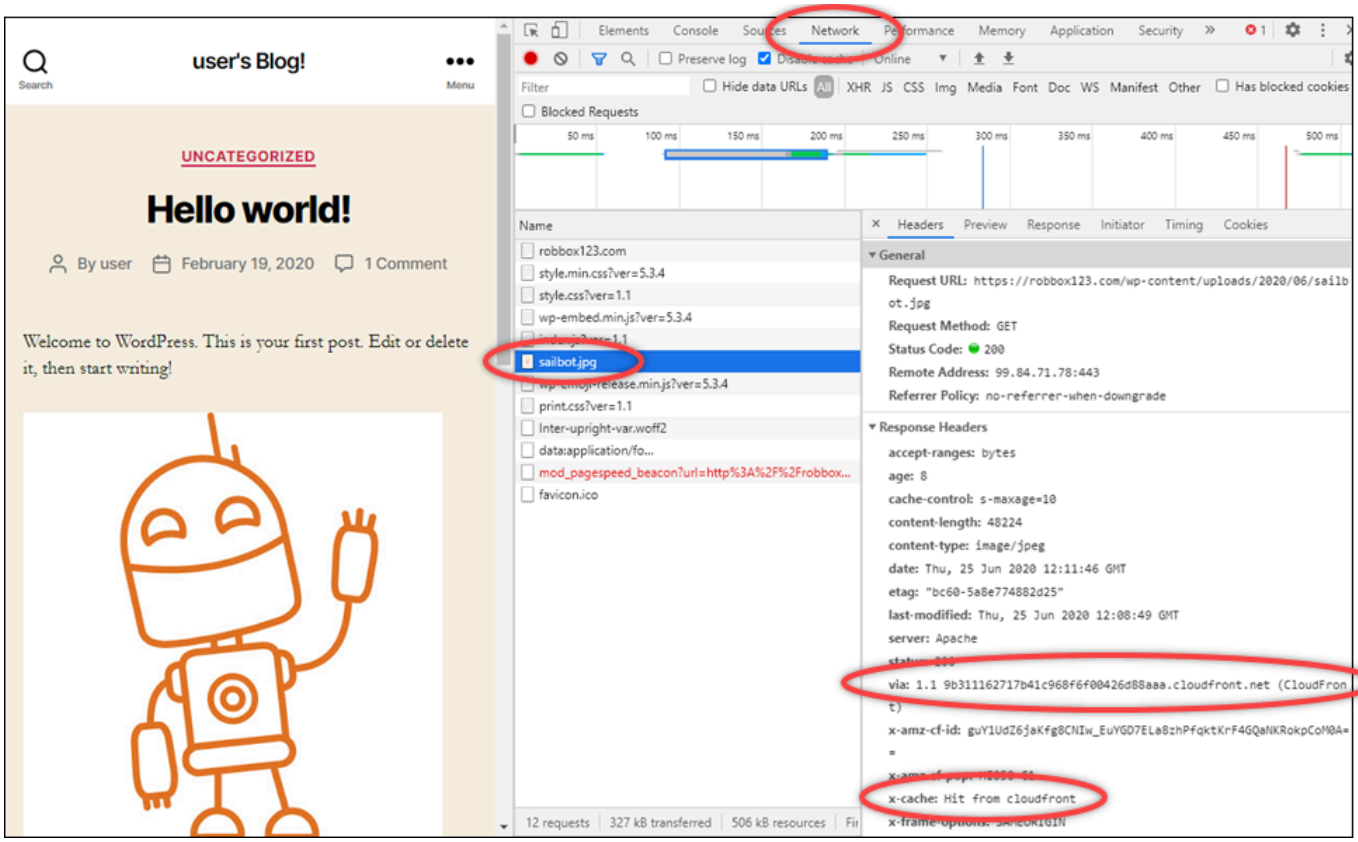
Testen Ihrer Verteilung

Vervollständigen Sie das folgende Verfahren, um einen Verteilung zu löschen. Wir verwenden in diesem Verfahren den Chrome-Webbrowser; andere Browser verwenden möglicherweise ähnliche Schritte.

1. Öffnen Sie den Chrome-Webbrowser.
2. Öffnen Sie Chrome-Menü in der oberen rechten Ecke des Browserfensters und wählen Sie Mehr Tools >Entwicklertools.

   Sie können auch die Tastenkombination Option + ⌘+ J (unter macOS) oder Umschalttaste + STRG + J (unter Windows/Linux) verwenden.
3. Wählen Sie im Bereich Entwicklertools die Registerkarte Netzwerk aus.
4. Navigieren Sie zu der Domain Ihrer Verteilung (z. B. `https://www.example.com`).

   Die Registerkarte Netzwerk der Chrome-Entwicklertools sollte mit einer Liste von Objekten von Ihrer Website gefüllt werden.
5. Wählen Sie ein statisches Objekt, z. B. eine Image-Datei (.jpg, .png, .gif).
6. Im Ereignisfenster Header, das angezeigt wird, sollten Sie sehen, dass die Header `via` und `x-cache` beide CloudFront erwähnen. Dadurch wird bestätigt, dass Ihre Verteilung Inhalte aus Ihrer Herkunft zwischenspeichert und bereitstellt.


user's Blog!
Search
Menu
UNCATEGORIZED
Hello world!
By user
February 19, 2020
1 Comment
Welcome to WordPress. This is your first post. Edit or delete it, then start writing!
Elements
Console
Network
Performance
Memory
Application
Security
Preserve log
Filter
Hide data URLs
XHR JS CSS Img Media Font Doc WS Manifest Other
Has blocked cookies
Blocked Requests
Name
robbox123.com
style.min.css?ver=5.3.4
style.css?ver=1.1
wp-embed.min.js?ver=5.3.4
sailbot.jpg
print.css?ver=1.1
Inter-upright-var.woff2
data:application/fo...
favicon.ico
Headers
Preview
Response
Initiator
Timing
Cookies
General
Request URL: https://robbox123.com/wp-content/uploads/2020/06/sailbot.jpg
Request Method: GET
Status Code: 200
Remote Address: 99.84.71.78:443
Referrer Policy: no-referrer-when-downgrade
Response Headers
accept-ranges: bytes
age: 8
cache-control: s-maxage=10
content-length: 48224
content-type: image/jpeg
date: Thu, 25 Jun 2020 12:11:46 GMT
etag: "bc60-5a8e774882d25"
last-modified: Thu, 25 Jun 2020 12:08:49 GMT
server: Apache
via: 1.1 9b311162717b41c968f6f00426d88aaa.cloudfront.net (CloudFront)
x-amz-cf-id: guY1UdZ6jaKfg8CNIw_EuYGD7ELa8zhPfqktKrF4GQaNKRokpCoM0A==
x-cache: Hit from cloudfront
12 requests
327 kB transferred
506 kB resources

Netzwerkressourcen in Amazon Lightsail

Lightsail-Netzwerkressourcen verbessern die Verbindung von Benutzern und externen Services zu Ihren Lightsail-Instances.

Load Balancers

Durch die Erstellung von Load Balancer können Sie mehr Redundanz hinzufügen oder mehr Datenverkehr bewältigen. Weitere Informationen finden Sie unter Load Balancer.

Statische IPs

Durch die Erstellung von statischen IP-Adressen können Sie bei jedem Neustart Ihrer Instance dieselbe IP-Adresse beibehalten. Weitere Informationen finden Sie unter Statische IP-Adressen.

Regionen und Availability Zones für Amazon Lightsail

Wenn Sie Ressourcen in Amazon Lightsail erstellen, erstellen Sie sie in einer AWS-Region, die Ihren Benutzern am nächsten ist. Beispiel: Wenn Ihr Blog-Datenverkehr zumeist aus der Schweiz kommt, wählen Sie Frankfurt oder Paris.

> **Note**
>
> DNS-Zonen sind globale Ressourcen. Sie werden nur in der Region USA Ost (Nord-Virginia) (us-east-1) erstellt, können aber auf jede Instance in jeder AWS-Region verweisen.

Lightsail ist in den folgenden AWS-Regionen verfügbar:

- USA Ost (Ohio): (us-east-2)
- USA Ost (Nord-Virginia): (us-east-1)
- USA West (Oregon): (us-west-2)
- Asien-Pazifik (Mumbai): (ap-south-1)
- Asien-Pazifik (Seoul): (ap-northeast-2)
- Asien-Pazifik (Singapur): (ap-southeast-1)
- Asien-Pazifik (Sydney): (ap-southeast-2)

- Asien-Pazifik (Tokyo) (ap-northeast-1)
- Kanada (Zentral): (ca-central-1)
- EU (Frankfurt): (eu-central-1)
- EU (Irland) (eu-west-1)
- EU (London): (eu-west-2)
- EU (Paris): (eu-west-3)
- EU (Stockholm) – eu-north-1

SSH-Schlüssel und Lightsail-Regionen

Sobald Sie in Lightsail eine Instance in einer AWS-Region erstellen, wird ein Standard-SSH-Schlüssel in dieser Region erstellt. Dieser Standardschlüssel kann verwendet werden, um eine Verbindung zu Instances nur in dieser bestimmten Region herzustellen. Um denselben Schlüssel in allen Regionen zu verwenden, in denen Sie Instances haben, erstellen Sie Ihr eigenes Schlüsselpaar und laden es in jede dieser Regionen hoch. Oder laden Sie ein bestehendes Schlüsselpaar in diesen Regionen hoch.

Weitere Informationen finden Sie unter SSH-Schlüsselpaare.

Tipps für die Arbeit mit Lightsail-Regionen

Jede AWS-Region ist so ausgelegt, dass sie vollständig von den anderen AWS-Regionen getrennt ist. Dies sorgt für die größtmögliche Fehlertoleranz und Stabilität.

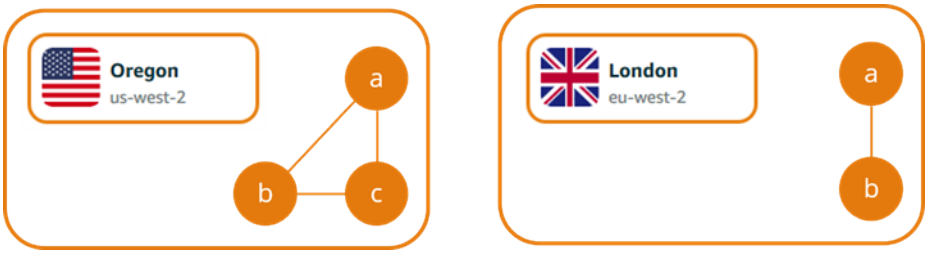
Die gesamte Kommunikation zwischen Regionen über das öffentliche Internet. Daher sollten Sie Ihre Daten mit entsprechenden Verschlüsselungsmethoden schützen. Beachten Sie, dass für die

Datenübertragung zwischen Regionen eine Gebühr anfällt. Weitere Informationen hierzu erhalten Sie unter Amazon EC2-Preise – Datenübertragung.

Wenn Sie mit einer Lightsail-Instance über die AWS Command Line Interface (AWS CLI) oder API-Vorgänge arbeiten, müssen Sie den regionalen Endpunkt angeben. Verwenden Sie die Option `--region` in Ihrem AWS CLI-Befehl und geben Sie `us-east-1` an, um Informationen zu DNS-Zonen und Netzwerk-Ressourcen zurückzugeben. Weitere Informationen zur Verwendung der AWS CLI-Option `--region` finden Sie unter Allgemeine Optionen in der AWS CLI-Referenz.

Lightsail-Availability-Zones

Availability Zones sind Gruppen von Rechenzentren, die auf einer physisch separierten, unabhängigen Infrastruktur ausgeführt werden. Availability Zones sind auf hohe Zuverlässigkeit ausgelegt. Generatoren oder Kühlsysteme, also mögliche Fehlerquellen, versorgen stets nur eine Availability Zone. Darüber hinaus sind Availability Zones physisch separiert, sodass selbst extrem unwahrscheinliche Katastrophen wie Feuer, Tornados oder Überflutungen jeweils nur die einzelne Availability Zone betreffen können, in der sie auftreten.



Jede AWS-Region hat zwei bis sechs Availability Zones, die durch einen Buchstaben nach dem Region-Namen gekennzeichnet sind (`us-east-2`*`a`*). Sie können jeweils nur eine Availability Zone in Lightsail-Instances erstellen. Sie sehen zu dem Zeitpunkt, zu dem Sie Ihre Instance erstellen, möglicherweise nicht alle Availability Zones. Wenn die Liste der Availability Zones nicht angezeigt wird, stellen Sie sicher, dass Sie im vorherigen Schritt eine Region ausgewählt haben.

Availability Zones und Ihre Lightsail-Anwendung

Indem Instances in separaten Availability Zones gestartet werden, können Sie Ihre Anwendungen vor den Fehlern eines einzelnen Standorts schützen.

Um eine Instance zu erstellen, die in mehreren Availability Zones verfügbar ist, erstellen Sie zunächst einen Snapshot Ihrer Instance. Als Nächstes wählen Sie eine andere Availability Zone, wenn Sie eine neue Instance aus dem erstellten Snapshot erstellen.

Weitere Informationen finden Sie unter AWS-Regionen-Regionen and Availability Zones im Amazon-EC2-Benutzerhandbuch.

Konfiguration von Reverse-DNS für einen E-Mail-Server auf Ihrer Amazon Lightsail-Instance

Ein Reverse Domain Name System (DNS) Lookup wird von E-Mail-Servern verwendet, um zu verfolgen, woher eine Nachricht stammt, und um zu bestätigen, dass sie kein Spam oder bösartig ist. Ein Reverse-DNS-Lookup gibt den Domänennamen einer IP-Adresse zurück. Ein Forward-DNS-Lookup gibt hingegen die IP-Adresse einer Domäne zurück.

Wenn beispielsweise ein Reverse-DNS-Lookup der IP-Adresse `192.168.1.2` die Subdomäne `mail.example.com` und ein Forward-DNS-Lookup der Subdomäne `mail.example.com` die IP-Adresse `192.168.1.2` zurückgibt, dann wird der Reverse-DNS für die IP-Adresse `192.168.1.2` "forward-confirmed". Weitere Informationen finden Sie unter Forward-confirmed reverse DNS auf Wikipedia.

Sie können Reverse-DNS für Ihre Amazon Lightsail-Instance konfigurieren, indem Sie die Voraussetzungen erfüllen und eine Anfrage an den AWS Support absenden, um Kontingente für ausgehende Nachrichten zu beseitigen. Diese Schritte werden in den folgenden Abschnitten behandelt.

Voraussetzungen

Um Reverse-DNS zu konfigurieren, müssen Sie die folgenden Voraussetzungen in der angezeigten Reihenfolge erfüllen:

1. Erstellen Sie eine Lightsail-Instance, die als E-Mail-Server verwendet werden soll. Weitere Informationen finden Sie unter Erstellen einer Instance.
2. Erstellen Sie eine statische IP, die für den Reverse-DNS-Eintrag verwendet werden soll, und hängen Sie sie an Ihre laufende Instance an. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

> **Important**
>
> Sie können die standardmäßige öffentliche IP, die einer Instance beim ersten Erstellen zugewiesen wird, nicht für Reverse DNS verwenden. Dies liegt daran, dass sich die

standardmäßige öffentliche IP-Adresse für Ihre Instance ändert, wenn Sie Ihre Instance stoppen und starten.

3. Fügen Sie in der DNS-Zone Ihrer Domäne einen Alias-Datensatz (A-Datensatz) hinzu, der für eine Subdomäne (z. B. `mail.example.com`) auf die statische IP-Adresse Ihrer laufenden Instance verweist. Dies ist die Subdomäne, die zurückgegeben wird, wenn ein Reverse-DNS-Lookup für die statische IP-Adresse durchgeführt wird. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.

   Note

   Wir empfehlen, dass Sie die Verwaltung der DNS-Datensätze Ihrer Domäne auf Lightsail übertragen. Auf diese Weise können Sie alle Ihre Ressourcen, einschließlich Ihrer Domäne, an einem einzigen Ort verwalten – der Lightsail-Konsole. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.

4. Warten Sie einige Zeit, damit sich Änderungen über das DNS im Internet ausbreiten. Anschließend können Sie die Anfrage an den AWS Support senden, um Reverse-DNS zu konfigurieren.

Senden einer Anfrage an den AWS Support, um Reverse-DNS zu konfigurieren

Aus Sicherheitsgründen begrenzt Lightsail ausgehende Nachrichten über Port 25 standardmäßig. Sie können jedoch den AWS Support bitten, dieses Kontingent aus Ihrem Konto zu entfernen und Reverse-DNS für Ihre statische IP zu konfigurieren.

So stellen Sie eine Anfrage an den AWS Support

1. Melden Sie sich in der Lightsail-Konsole als AWS-Konto-Stammbenutzer an.

   Important

   Die Anforderung muss mit dem AWS-Konto-Stammbenutzer eingereicht werden. Weitere Informationen über den AWS-Konto-Stammbenutzer finden Sie unter Der Stammbenutzer des AWS-Kontos.

2. Navigieren Sie zum Formular Anforderung zum Entfernen von E-Mail-Sendebeschränkungen und geben Sie die folgenden erforderlichen Informationen ein:

> **Note**
>
> Das Formular verweist auf Amazon Elastic Compute (EC2)-Ressourcen (wie z. B. Elastic IPs (EIPs) und EC2-Instances). Sie können das Formular aber auch für Ihre Lightsail-Ressourcen wie statische IPs und Lightsail-Instances verwenden.

- E-Mail-Adresse – Geben Sie die E-Mail-Adresse ein, unter der Sie Nachrichten zu Ihrer Anfrage erhalten können. Die E-Mail-Adresse Ihres Kontos ist in diesem Textfeld bereits eingetragen.
- Anwendungsfallbeschreibung – Geben Sie den Grund für die Entfernung des E-Mail-Kontingents an.
- Elastic IP-Adresse – Geben Sie die statische IP-Adresse ein, die Sie Ihrer Instance in Schritt 2 der Voraussetzungen zuvor in diesem Handbuch zugewiesen haben. Sie können bis zu zwei statische IP-Adressen eingeben.
- Reverse-DNS-Eintrag für EIP – Geben Sie die Subdomäne ein, die Sie in Schritt 3 der Voraussetzungen zuvor in diesem Handbuch definiert haben. Dies ist die Domäne, die zurückgegeben wird, wenn das Reverse-DNS-Lookup durchgeführt wird.

3. Wählen Sie Submit (Senden) aus, wenn Sie fertig sind.

Nachdem Ihre Anfrage vom AWS Support abgeschlossen wurde, kann Ihre statische IP-Adresse mit Reverse-DNS-Lookup bestätigt werden.

Wenn Sie die statische IP-Adresse später aus Ihrem Lightsail-Konto löschen möchten, müssen Sie eine Anfrage an den AWS Support senden, um die Reverse-DNS-Konfiguration zu entfernen. Nachdem die Reverse-DNS-Konfiguration entfernt wurde, können Sie die statische IP-Adresse über die Lightsail-Konsole aus Ihrem Lightsail-Konto löschen. Weitere Informationen finden Sie unter Löschen einer statischen IP.

Einrichten von Amazon-VPC-Peering für die Zusammenarbeit mit AWS-Ressourcen außerhalb von Amazon Lightsail

Lightsail ermöglicht Ihnen, über ein Peering der Virtual Private Cloud (VPC) eine Verbindung zu AWS-Ressourcen herzustellen, wie beispielsweise zu einer Amazon-RDS-Datenbank. Eine VPC ist ein virtuelles Netzwerk, das speziell für Ihr AWS-Konto ausgelegt ist. Alles, was Sie in Lightsail erstellen, befindet sich in einer VPC, und Sie können Ihre Lightsail-VPC mit einer Amazon VPC verbinden.

Einige AWS-Ressourcen, wie Amazon S3, Amazon CloudFront und Amazon DynamoDB, benötigen kein VPC-Peering für die Aktivierung.

> **Note**
>
> Zum Aktivieren des VPC-Peerings in Lightsail brauchen Sie eine Standard-Amazon-VPC. Wenn Sie nicht über eine standard Amazon VPC verfügen, können Sie eine erstellen. Weitere Informationen finden Sie unter Erstellen einer Standard-VPC im Benutzerhandbuch zu Amazon VPC.
> Da AWS-Regionen voneinander isoliert sind, ist auch eine VPC in der Region isoliert, in der Sie erstellt wurde. Sie müssen das VPC-Peering in jeder Region aktivieren, in der Sie Lightsail-Ressourcen haben.

Sobald Sie über eine Standard-Amazon-VPC verfügen, führen Sie die folgenden Anweisungen aus, um Ihre Lightsail-VPC mit Ihrer Amazon VPC zu koppeln.

1. Wählen Sie in der Lightsail-Konsole im oberen Navigationsmenü Account (Konto) aus.
2. Wählen Sie Account (Konto) aus dem Dropdown-Menü.
3. Wählen Sie die Registerkarte Advanced.
4. Wählen Sie VPC-Peering aktivieren für die AWS-Region aus, in der Sie es aktivieren möchten.

Wenn die Peering-Verbindung fehlschlägt, versuchen Sie erneut, das VPC-Peering zu aktivieren. Wenn dies nicht funktioniert, wenden Sie sich bitte an den AWS-Kundenservice.

Eine Peering-Verbindung wird in Ihrem AWS-Konto erstellt, wenn die Peering-Anfrage erfolgreich ist. Rufen Sie das Amazon-VPC-Dashboard auf und wählen Sie Peering-Verbindungen im Navigationsbereich, um die erstellte Peering-Verbindung anzuzeigen.

Weitere Informationen zu Amazon VPC finden Sie unter Ihre VPC und Subnetze im Benutzerhandbuch zu Amazon VPC.

IP-Adressen in Amazon Lightsail

Sie können über ihre IP-Adressen mit Ihrer Lightsail-Instance und anderen Lightsail-Ressourcen kommunizieren. Wenn Sie beispielsweise die öffentliche IP-Adresse Ihrer Instance verwenden, können Sie den Netzwerkstatus Ihrer Instance überprüfen (mithilfe von PING), eine SSH-Verbindung zu Ihrer Instance herstellen und Datenverkehr von einem benutzerdefinierten Domänennamen an Ihre Instance weiterleiten. Es gibt noch viele weitere Dinge, die Sie mit der IP-Adresse Ihrer Lightsail-Ressourcen tun können.

Lightsail-Instances, Container-Services und Load Balancer unterstützen sowohl die IPv4- als auch die IPv6-Adressierungsprotokolle. Standardmäßig verwenden, und das IPv4-Adressierungsprotokoll; dieses Verhalten lässt sich nicht deaktivieren. Sie können optional IPv6 für Ihre Instances, Container-Services und Load Balancer aktivieren.

In diesem Leitfaden behandeln wir, was Sie über IP-Adressen in Lightsail wissen müssen.

Inhalt

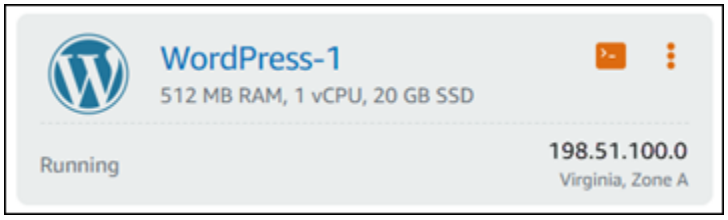
Private und öffentliche IPv4-Adressen

Wenn Sie eine Lightsail-Instance erstellen, wird ihr eine öffentliche und eine private IPv4-Adresse zugewiesen. Die öffentliche IP-Adresse ist für das Internet zugänglich, während die private IP-Adresse nur für Ressourcen in Ihrem Lightsail-Konto in derselben zugänglich istAWS-Region.

> **Note**
>
> Die private IP-Adresse Ihrer Instance kann für andere AWS-Ressourcen in derselben AWS-Region, jedoch außerhalb Ihres Lightsail-Kontos, zugänglich sein, wenn Sie VPC-Peering aktivieren. Weitere Informationen finden Sie unter Einrichten von Amazon VPC Peering für die Zusammenarbeit mit AWS-Ressourcen außerhalb von Lightsail.

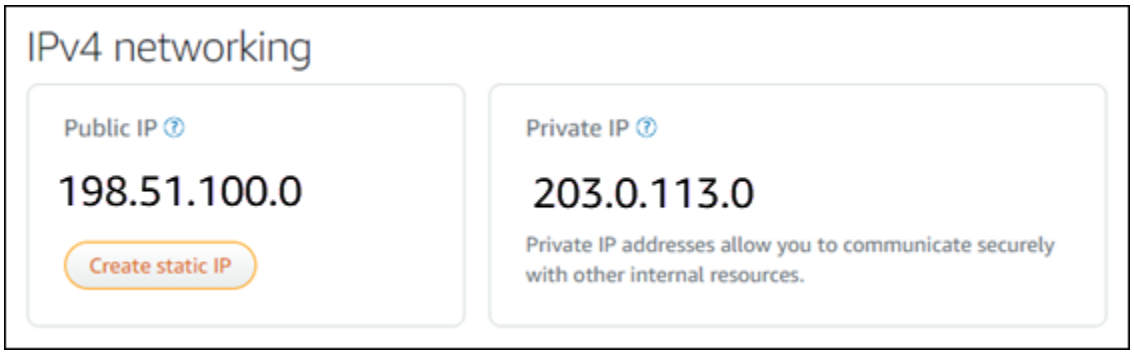
Die IP-Adressen Ihrer Instance werden in den folgenden Bereichen der Lightsail-Konsole angezeigt:

- Das folgende Beispiel zeigt die öffentliche IP-Adresse einer Instance auf der Lightsail-Startseite.



- Das folgende Beispiel zeigt die öffentlichen und privaten IP-Adressen einer Instance im Header-Bereich der Instance-Verwaltungsseite.

- Das folgende Beispiel zeigt die öffentlichen und privaten IP-Adressen einer Instance auf der Netzwerkfunktionen, die Registerkarte der Instance-Verwaltungsseite.



Beachten Sie bei Verwendung der IPv4-Adressen Ihrer Instances Folgendes:

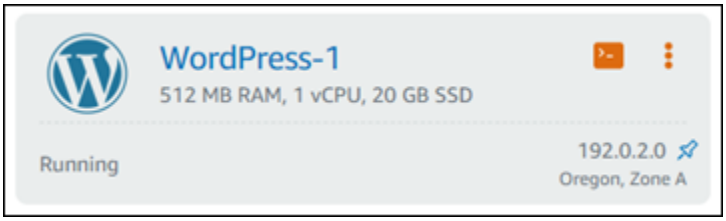
- Rufen Sie die öffentliche IP-Adresse Ihrer Instance ab. Geben Sie Ihrer Instance eine IP-Adresse an, die sich nie ändert, indem Sie eine statische IP-Adresse hinzufügen. Weitere Informationen finden Sie unter dem Statische IP-Adressen für Instances-Abschnitt in diesem Handbuch.
- Lightsail verwendet standardmäßig IPv4-Adressen. Sie können IPv6 jedoch optional für einige Lightsail-Ressourcen aktivieren, die vor dem 12. Januar 2021 erstellt wurden. Für Ressourcen, die am oder nach dem 12. Januar 2021 erstellt wurden, ist IPv6 standardmäßig aktiviert. Weitere Informationen finden Sie im Abschnitt IPv6 für Instances, Containerdienste, CDN-Verteilungen und Load Balancers in diesem Handbuch.
- Sie können der Firewall für Ihre -Instance Regeln hinzufügen, um den Datenverkehr zu steuern, der eine Verbindung dazu herstellen darf. Weitere Informationen finden Sie unter Instance-Firewalls.

Statische IPv4-Adressen für Instances

Die standardmäßige öffentliche IPv4-Adresse, die Ihrer Instance beim Erstellen zugewiesen wird, ändert sich beim Anhalten und Starten Ihrer Instance. Sie können optional eine statische IPv4-Adresse erstellen und an Ihre Instance anfügen. Die statische IPv4-Adresse ersetzt die standardmäßige öffentliche IPv4-Adresse Ihrer Instanz und bleibt unverändert, wenn Sie die Instance anhalten und starten. Sie können eine statische IP an eine Instance anhängen. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

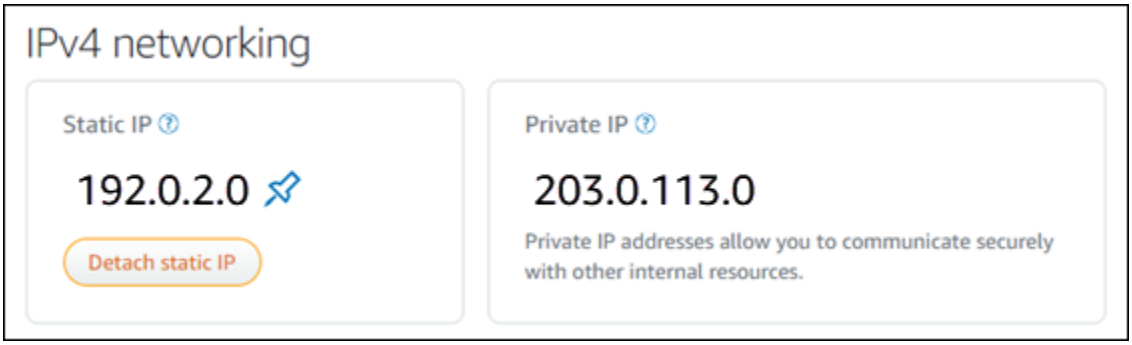
Nachdem Sie eine statische IP erstellt und an Ihre Instance angehängt haben, wird sie in den folgenden Bereichen der Lightsail-Konsole angezeigt:

- Das folgende Beispiel zeigt die statische IP-Adresse einer Instance auf der Lightsail-Startseite. Das Thumbtack-Symbol bedeutet, dass die öffentliche IP-Adresse statisch ist.

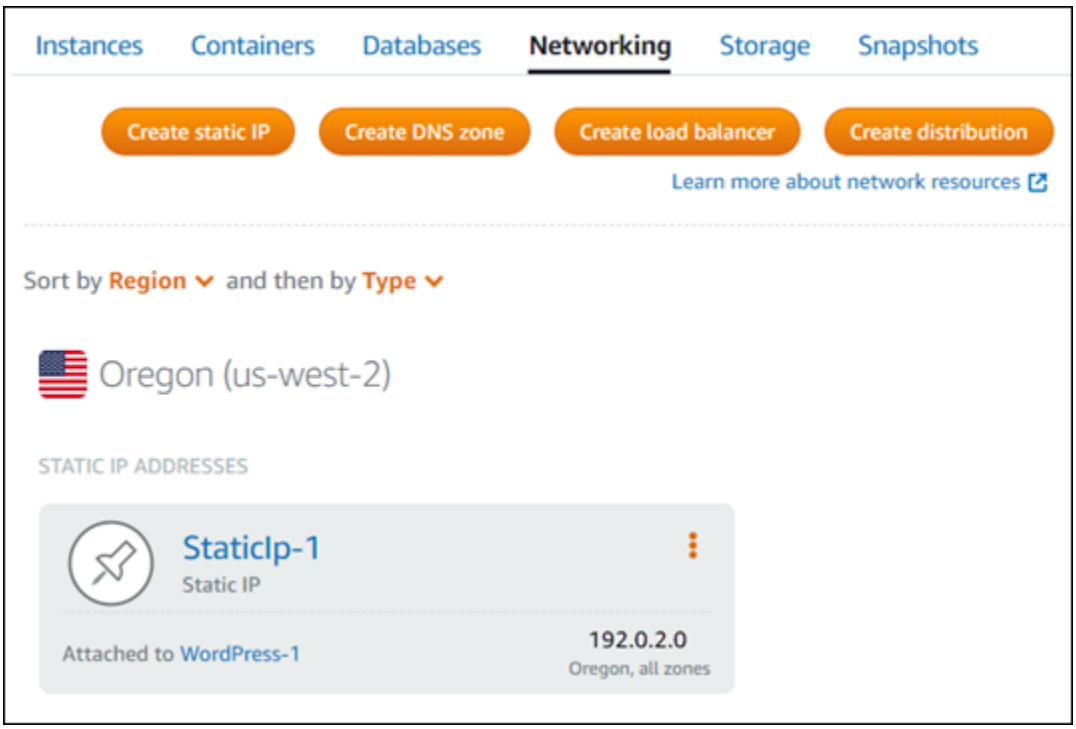


- Das folgende Beispiel zeigt die statische IP-Adresse einer Instance im Headerbereich der Instanzverwaltungsseite. Das Thumbtack-Symbol bedeutet, dass die öffentliche IP-Adresse statisch ist.

- Das folgende Beispiel zeigt die statische IP-Adresse einer Instance auf der Netzwerkfunktionen, die Registerkarte der Instance-Verwaltungsseite. Die öffentliche Standardadresse ist nicht mehr aufgeführt und wurde durch die statische IP-Adresse ersetzt. Das Thumbtack-Symbol bedeutet, dass die öffentliche IP-Adresse statisch ist.



- Sie können alle statischen IPs anzeigen, die Sie erstellt haben, indem Sie die Registerkarte Netzwerk der Lightsail-Startseite aufrufen, wie im folgenden Beispiel gezeigt.



IPv6 für Instances, Containerdienste, CDN-Verteilungen und Load Balancers

IPv6 ist standardmäßig für Lightsail-Instances, Container-Services, CDN-Verteilungen und Load Balancer aktiviert, die am oder nach dem 12. Januar 2021 erstellt wurden. Sie können optional IPv6 für die Ressourcen aktivieren, die vor dem 12. Januar 2021 erstellt wurden. Wenn Sie IPv6 für eine bestimmte Ressource aktivieren, weist Lightsail dieser Ressource automatisch eine IPv6-Adresse zu. Sie können die IPv6-Adresse nicht selbst auswählen oder angeben. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren von IPv6.

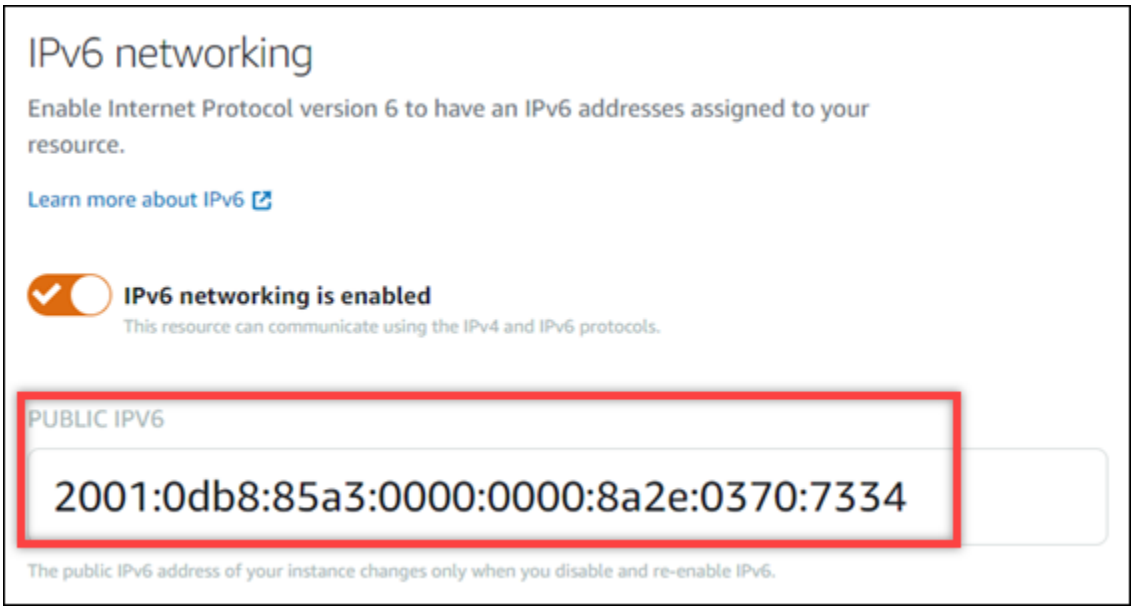
Sie können auch eine IPv6-onlyInstance erstellen. Eine IPv6-onlyInstance kann nur über IPv6 öffentlich kommunizieren und hat keine öffentliche IPv4-Adresse. Weitere Informationen finden Sie unter IPv6-onlyInstance-Pläne in Lightsail.

Die IPv6-Adresse Ihrer Instance wird in den folgenden Bereichen der Lightsail-Konsole angezeigt:

- Das folgende Beispiel zeigt die IPv6-Adresse einer Instance auf der Lightsail-Startseite.

- Das folgende Beispiel zeigt die IPv6-Adresse einer Ressource im Kopfzeilenbereich der Verwaltungsseite der Ressource.

- Das folgende Beispiel zeigt die IPv6-Adresse einer Ressource auf der Registerkarte Netzwerk der Seite Ressourcenverwaltung.



Beachten Sie Folgendes, wenn Sie IPv6 für Ihre Ressourcen aktivieren und verwenden:

- Ihre Ressourcen können über IPv4 und IPv6 (im Dual-Stack-Modus) kommunizieren, wenn Sie IPv6 für eine Ressource aktivieren, oder nur über IPv4.

- Wenn Sie IPv6 für eine Ressource aktivieren, weist Lightsail dieser Ressource automatisch eine IPv6-Adresse zu. Sie können die IPv6-Adresse nicht selbst auswählen oder angeben. Wenn Sie IPv6 für eine Ressource aktivieren, beginnt es, Netzwerkverkehr über das IPv6-Protokoll zu akzeptieren.
- Die IPv6-Adresse für eine Instance bleibt beim Anhalten und Starten Ihrer Instance bestehen. Es wird nur veröffentlicht, wenn Sie Ihre Instance löschen oder IPv6 für Ihre Instance deaktivieren. Sie können die IPv6-Adresse nicht wieder abrufen, nachdem Sie eine dieser Aktionen ausgeführt haben.
- Alle IPv6-Adressen, die Ihren Instances zugewiesen sind, sind öffentlich und über das Internet erreichbar. Es gibt keine privaten IPv6-Adressen, die Ihren Instances zugewiesen sind.
- IPv4- und IPv6-Adressen für Instances sind voneinander unabhängig. Sie müssen daher die Instance-Firewallregeln für IPv4 und IPv6 getrennt konfigurieren. Weitere Informationen finden Sie unter Instance-Firewalls.
- Nicht alle in Lightsail verfügbaren Instance-Vorlagen werden automatisch für IPv6 konfiguriert, wenn IPv6 aktiviert ist. Instances, die die folgenden Blueprints verwenden, erfordern zusätzliche Konfigurationsschritte, nachdem Sie IPv6 für sie aktiviert haben:
  - cPanel – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf cPanel-Instances.
  - Debian 8 – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Debian-8-Instances.
  - GitLab – Weitere Informationen finden Sie unter Konfigurieren von IPv6 für GitLab Instances.
  - Nginx – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Nginx-Instances.
  - Plesk – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Plesk-Instances.
  - Ubuntu 16 – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Ubuntu-16-Instances.

> **Note**
>
> PrestaShop unterstützt derzeit keine IPv6-Adressen. Sie können IPv6 für die Instance aktivieren, aber die PrestaShop Software reagiert nicht auf Anfragen über das IPv6-Netzwerk.

Statische IP-Adressen in Amazon Lightsail

Eine statische IP ist eine feste, öffentliche IP-Adresse, die Sie einer Instance oder anderen Ressource zuweisen. Wenn Sie keine statische IP-Adresse einrichten, weist Lightsail Ihrer Instance nach jedem Anhalten und Neustarten eine neue öffentliche IP-Adresse zu.

> **Important**
>
> Wenn Sie Ihre Instance stoppen oder neu starten, ohne zunächst eine statische IP-Adresse einzurichten und an Ihre Instance anzufügen, verlieren Sie Ihre IP-Adresse, wenn Ihre Instance neu gestartet wird. Sie sollten eine statische IP-Adresse erstellen und an Ihre Instance anfügen, um sicherzustellen, dass Ihre Instance immer dieselbe öffentliche IP-Adresse hat. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse.

Inhalt

Erstellen einer statischen IP-Adresse und Anfügen an eine Lightsail-Instance

Die standardmäßige dynamische öffentliche IP-Adresse, die Ihrer Amazon Lightsail-Instance zugeordnet ist, ändert sich jedes Mal, wenn Sie die Instance anhalten und neu starten. Erstellen Sie eine statische IP-Adresse und fügen Sie sie an Ihre Instance an, damit die öffentliche IP-Adresse nicht mehr geändert wird. Wenn Sie später einen registrierten Domänennamen Ihrer Instance zuweisen, müssen Sie nicht jedes Mal, wenn Sie Ihre Instance stoppen und neu starten, die DNS-Datensätze Ihrer Domäne aktualisieren. Sie können eine statische IP an eine Instance anhängen. Weitere Informationen finden Sie unter Statische IP-Adressen.

Voraussetzungen

Sie benötigen mindestens eine Dual-Stack-Instance, die in Lightsail ausgeführt wird. Um eine zu erstellen, lesen Sie unter Eine Instance erstellen nach.

Eine statische IP-Adresse erstellen und einer Instance zuordnen

Gehen Sie wie folgt vor, um eine neue statische IP-Adresse zu erstellen und sie an eine Instance in Lightsail anzuhängen.

1. Melden Sie sich bei der Lightsail-Konsole unter https://lightsail.aws.amazon.com/ an.
2. Wählen Sie auf der Lightsail-Startseite Netzwerk aus.
3. Wählen Sie Create static IP (Statische IP erstellen) aus.
4. Wählen Sie die AWS-Region, in der Sie Ihre statische IP erstellen möchten.

   > **Note**
   >
   > Statische IP-Adressen können nur Instances in derselben Region angefügt werden.

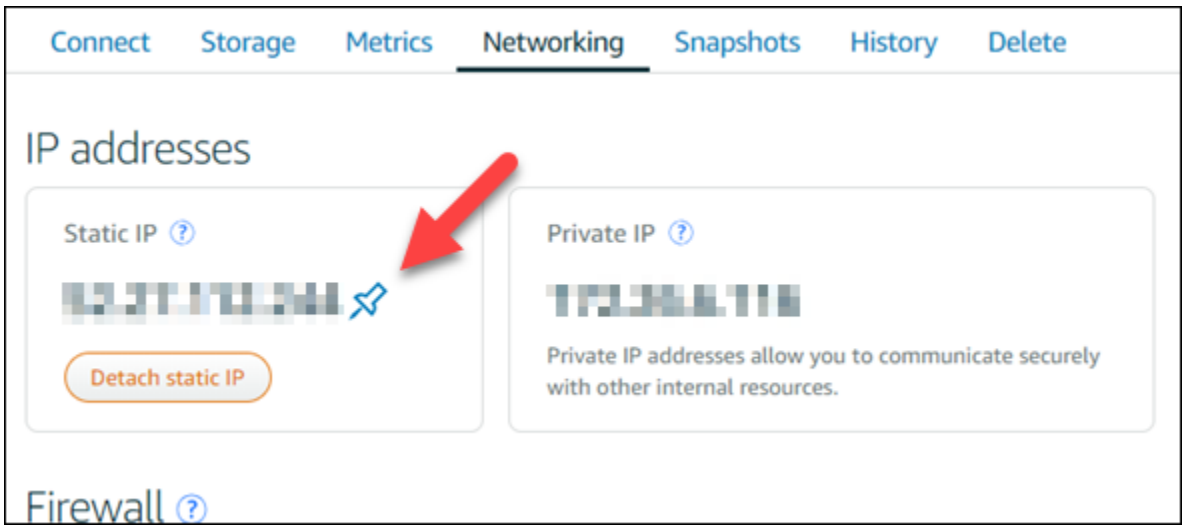
5. Wählen Sie die Lightsail-Ressource aus, an die Sie die statische IP anfügen möchten.
6. Geben Sie einen Namen für Ihre statische IP ein.

   Ressourcennamen:

   - Muss in jedem AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.
7. Wählen Sie Erstellen.

   Jetzt sehen Sie auf der Website eine statische IP-Adresse, die Sie verwalten können.

   Auf der Registerkarte Networking (Netzwerk) Ihrer Instance-Verwaltungsseite sehen Sie einen blauen Pin neben Ihrer öffentlichen IP-Adresse. Daran erkennen Sie, dass die IP-Adresse ist jetzt statisch.



Weitere Informationen finden Sie unter Öffentliche IP-Adressen und private IP-Adressen.

Löschen einer statischen IP-Adresse in Lightsail

Sie können bis zu fünf statische IPs pro AWS-Region in Ihrem Amazon Lightsail-Konto erstellen. Wenn Sie eine Instance löschen, an die eine statische IP-Adresse angehängt ist, verbleibt die statische IP-Adresse in Ihrem Konto. Wenn Sie die statische IP-Adresse nicht mehr benötigen, können Sie sie mithilfe der Lightsail-Konsole oder der AWS Command Line Interface () löschenAWS CLI. In diesem Leitfaden zeigen wir Ihnen, wie Sie eine statische IP-Adresse aus Ihrem Lightsail-Konto löschen. Weitere Informationen über statische IPs finden Sie unter IP-Adressen.

> **Important**
>
> Durch das Löschen einer statischen IP wird die statische IP vollständig aus Ihrem Lightsail-Konto entfernt. Ressourcen, die diese statische IP verwenden, wie Instances, sind davon betroffen. Sie können die statischen IP nicht mehr zurückerhalten, nachdem Sie sie gelöscht haben.

Löschen einer statischen IP mithilfe der Lightsail-Konsole

Führen Sie das folgende Verfahren aus, um eine statische IP mithilfe der Lightsail-Konsole zu löschen.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite Netzwerk aus.

3. Wählen Sie auf der Seite Netzwerk das vertikale Ellipsensymbol (⋮) neben der statischen IP-Adresse aus, die Sie löschen möchten, und wählen Sie dann Löschen aus.

Löschen Sie eine statischen IP unter Verwendung der AWS CLI

Führen Sie die folgenden Schritte aus, um eine statische IP mit der AWS CLI zu löschen. Der Befehl zum Löschen einer statischen IP aus Ihrem Lightsail-Konto lautet release-static-ip. Wenn Sie eine statische IP erstellen, weisen Sie sie eigentlich zu. Statt also die statische IP zu löschen, geben Sie sie eigentlich frei.

Voraussetzungen

Falls noch nicht passiert, müssen Sie die AWS CLI installieren. Weitere Informationen finden Sie unter Installieren der AWS Command Line Interface. Achten Sie drauf, die AWS CLI zu konfigurieren.

Sie müssen den Namen Ihrer statischen IP kennen, um sie freigeben zu können. Dazu verwenden Sie den AWS CLI-Befehl `get-static-ips`.

1. Geben Sie den folgenden Befehl ein:

```
aws lightsail get-static-ips
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "staticIps": [
        {
            "name": "Example-StaticIP",
            "resourceType": "StaticIp",
            "attachedTo": "MyInstance",
            "arn": "arn:aws:lightsail:us-east-2:123456789101:StaticIp/5282f35e-
c720-4e5a-1234-12345EXAMPLE",
```

```
            "isAttached": true,
            "ipAddress": "192.0.2.0",
            "createdAt": 1489750629.026,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-east-2"
            }
        },
        {
            "name": "my-other-static-ip",
            "resourceType": "StaticIp",
            "arn": "arn:aws:lightsail:us-east-2:123456789101:StaticIp/
f5885e14-8984-49e5-1234-12345EXAMPLE",
            "isAttached": false,
            "ipAddress": "192.0.2.2",
            "createdAt": 1483653597.815,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-east-2"
            }
        }
    ]
}
```

2. Wählen Sie den Name-Wert der statischen IP, die Sie freigeben wollen, und notieren Sie ihn, sodass Sie ihn im nächsten Schritt verwenden können.

   Sie können beispielsweise den Wert in die Zwischenablage kopieren.

3. Geben Sie den folgenden Befehl ein:

   ```
   aws lightsail release-static-ip --static-ip-name StaticIpName
   ```

   Ersetzen Sie im Befehl durch *`StaticIpName`* den Namen Ihrer statischen IP.

   Wenn Sie erfolgreich waren, sollte die Ausgabe folgendermaßen oder ähnlich aussehen.

   ```
   {
       "operations": [
           {
               "status": "Succeeded",
               "resourceType": "StaticIp",
               "isTerminal": true,
   ```

```
            "statusChangedAt": 1489860944.19,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-east-2"
            },
            "operationType": "ReleaseStaticIp",
            "resourceName": "Example-StaticIP",
            "id": "92a2f0d2-eef2-4e6f-1234-12345EXAMPLE",
            "createdAt": 1489860944.19
        }
    ]
}
```

Aktivieren und deaktivieren von IPv6 in Amazon Lightsail

IPv6 ist standardmäßig für Lightsail-Instances, Containerdienste, CDN-Verteilungen und Load Balancers, die am oder nach dem 12. Januar 2021 erstellt wurden. Sie können optional IPv6 für die Ressourcen aktivieren, die vor dem 12. Januar 2021 erstellt wurden. In diesem Leitfaden zeigen wir Ihnen, wie Sie IPv6 aktivieren oder deaktivieren. Weitere Informationen über IPv6 finden Sie unter IP-Adressen.

Inhalt

Überlegungen zu IPv6

IPv6 wurde inLightsailam 12. Januar 2021 verfügbar. Daher müssen Sie möglicherweise IPv6 für einige Ihrer Ressourcen manuell aktivieren oder deaktivieren, entsprechend dem folgenden Leitfaden:

- Für Instances, CDN-Verteilungen und Lastenverteilungen, dievordem 12. Januar erstellt wurden, ist IPv6 deaktiviert, bis Sie es aktivieren. Für Instances, CDN-Verteilungen und Lastenverteilungen, die jedochnachdem 12. Januar erstellt wurden, ist IPv6 aktiviert, wenn sie erstellt werden.
- Für Containerdienste, die vor oder nach dem 12. Januar erstellt wurden, ist IPv6 aktiviert.

- IPv6 kann für Instances, CDN-Verteilungen und Lastenverteilungsdienste jederzeit manuell aktiviert oder deaktiviert werden. Sie kann nicht für Containerdienste deaktiviert werden.

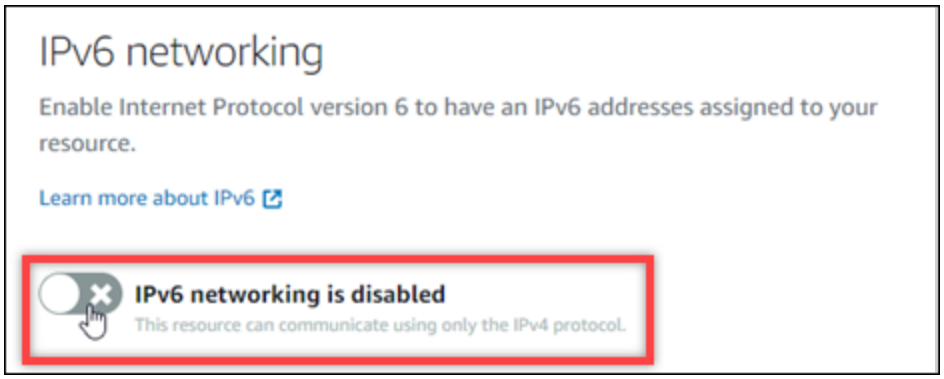
Beachten Sie bei der Aktivierung und Verwendung von IPv6 Folgendes:

- Ihre Ressourcen können nur über IPv4 oder über IPv4 und IPv6 (im Dual-Stack-Modus) kommunizieren, wenn Sie IPv6 für eine Ressource aktivieren.
- Wenn Sie IPv6 für eine Instance aktivieren, weist Lightsail dieser Instance automatisch eine IPv6-Adresse zu. Sie können die IPv6-Adresse nicht selbst auswählen oder angeben. Wenn Sie IPv6 für einen Containerdienst, eine CDN-Verteilung oder einen Lastenverteilungsdienst aktivieren, nimmt diese Ressource Internetverkehr über IPv6 an.
- Die IPv6-Adresse für eine Instance bleibt beim Anhalten und Starten Ihrer Instance bestehen. Es wird nur veröffentlicht, wenn Sie Ihre Instance löschen oder IPv6 für Ihre Instance deaktivieren. Sie können die IPv6-Adresse nicht wieder abrufen, nachdem Sie eine dieser Aktionen ausgeführt haben.
- Alle IPv6-Adressen, die Ihren Instances zugewiesen sind, sind öffentlich und über das Internet erreichbar. Es gibt keine privaten IPv6-Adressen, die Ihren Instances zugewiesen sind.
- IPv4- und IPv6-Adressen für Instances sind voneinander unabhängig. Sie müssen daher die Instance-Firewallregeln für IPv4 und IPv6 getrennt konfigurieren. Weitere Informationen finden Sie unter Instance-Firewalls.
- Nicht alle Instance-Blueprints, die in Lightsail werden automatisch für IPv6 konfiguriert, wenn IPv6 aktiviert ist. Instances, die die folgenden Blueprints verwenden, erfordern zusätzliche Konfigurationsschritte, nachdem Sie IPv6 für sie aktiviert haben:
  - cPanel – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf cPanel-Instances.
  - Debian 8 – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Debian-8-Instances.
  - GitLab – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf GitLab-Instances.
  - Nginx – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Nginx-Instances.
  - Plesk – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Plesk-Instances.
  - Ubuntu 16 – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Ubuntu-16-Instances.

IPv6 aktivieren

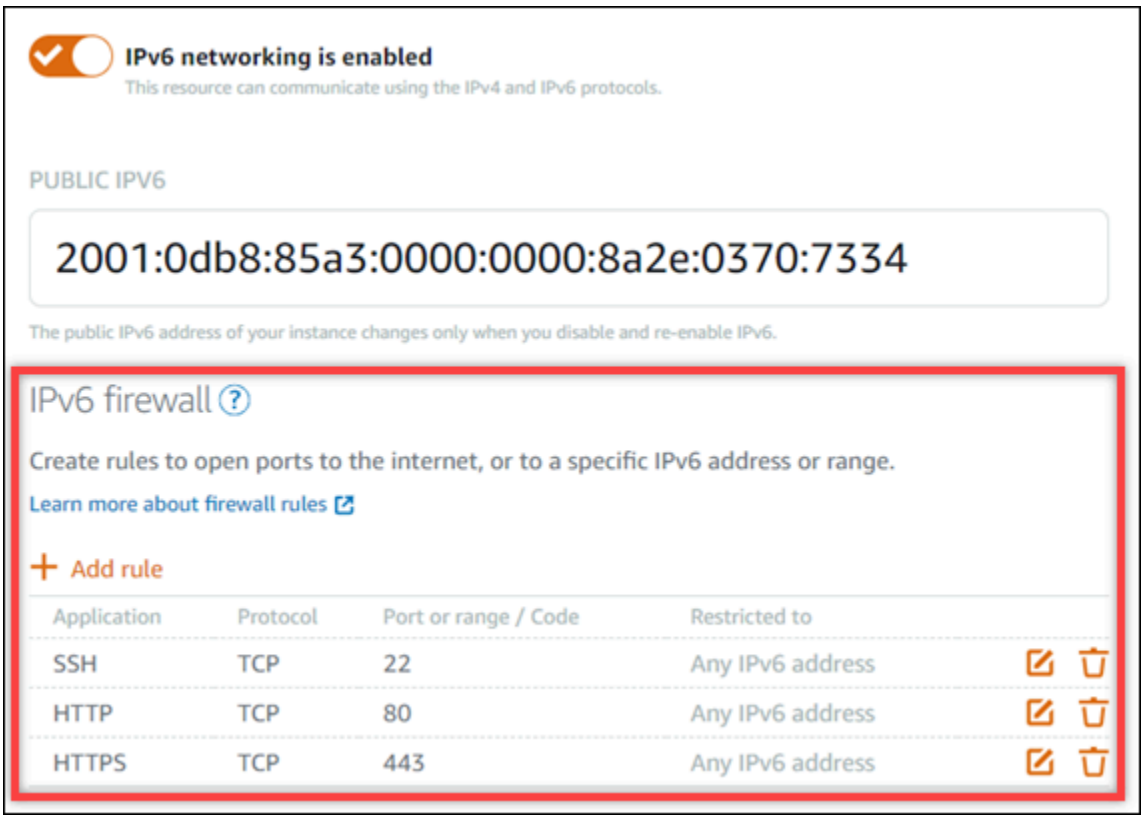
Vervollständigen Sie das folgende Verfahren, um IPv6 für Instances, CDN-Verteilungen und Lastenverteilungsdienste zu aktivieren.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Vervollständigen Sie je nach Ressource, für die Sie IPv6 aktivieren möchten, einen der folgenden Schritte:
   - Um IPv6 für eine Instance zu aktivieren, wählen Sie die Registerkarte Instances auf der Lightsail-Startseite und wählen Sie dann den Namen der Instance aus, für die Sie IPv6 aktivieren möchten.
   - Um IPv6 für eine CDN-Verteilung oder einen Load Balancer zu aktivieren, wählen Sie die Registerkarte Netzwerkfunktionen auf der Lightsail-Startseite und wählen Sie dann den Namen der CDN-Verteilung oder des Load Balancers aus, für die/den Sie IPv6 aktivieren möchten.
3. Wählen Sie die Registerkarte Netzwerkfunktionen auf der Verwaltungsseite der Ressource aus.
4. Im Abschnitt IPv6-Netzwerk der Seite wählen Sie den Schalter, um IPv6 für die Ressource zu aktivieren.



Beachten Sie die folgenden Elemente, nachdem Sie IPv6 für eine Ressource aktivieren:

- Wenn Sie IPv6 für eine CDN-Verteilung oder einen Lastenverteilungsdienst aktivieren, fängt diese Ressource an, Internetverkehr über IPv6 anzunehmen. Wenn Sie IPv6 für eine Instance aktivieren, wird ihr eine IPv6-Adresse zugewiesen, und die IPv6-Firewall wird verfügbar, wie im folgenden Beispiel gezeigt.

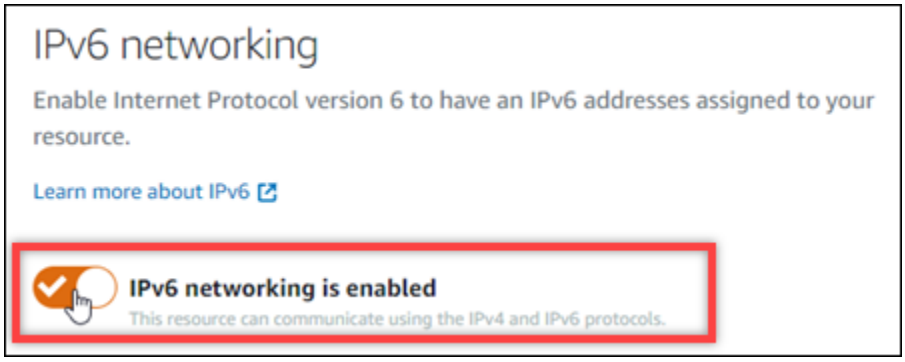


- Instances, die die folgenden Blueprints verwenden, erfordern nach der Aktivierung von IPv6 zusätzliche Schritte, um sicherzustellen, dass die Instance über ihre neue IPv6-Adresse informiert wird:
  - cPanel – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf cPanel-Instances.
  - Debian 8 – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Debian-8-Instances.
  - GitLab – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf GitLab-Instances.
  - Nginx – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Nginx-Instances.
  - Plesk – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Plesk-Instances.
  - Ubuntu 16 – Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Ubuntu-16-Instances.
- Wenn Sie über einen registrierten Domainnnamen verfügen, der Datenverkehr an Ihre Instance, den Containerdienst, die CDN-Verteilung oder die Load Balancer weiterleitet, müssen Sie im DNS Ihrer Domain eine IPv6-Adressakte (AAAA) erstellen, um IPv6-Datenverkehr an Ihre Ressource weiterzuleiten.

IPv6 deaktivieren

Vervollständigen Sie das folgende Verfahren, um IPv6 für Instances, CDN-Verteilungen und Lastenverteilungsdienste zu deaktivieren.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Vervollständigen Sie je nach Ressource, für die Sie IPv6 deaktivieren möchten, einen der folgenden Schritte:
   - Um IPv6 für eine Instance zu deaktivieren, wählen Sie die Registerkarte Instances auf der Lightsail-Startseite und wählen Sie dann den Namen der Instance aus, für die Sie IPv6 deaktivieren möchten.
   - Um IPv6 für eine CDN-Verteilung oder einen Load Balancer zu deaktivieren, wählen Sie die Registerkarte Netzwerkfunktionen auf der Lightsail-Startseite und wählen Sie dann den Namen der CDN-Verteilung oder des Load Balancers aus, für die/den Sie IPv6 deaktivieren möchten.
3. Wählen Sie die Registerkarte Netzwerkfunktionen auf der Verwaltungsseite der Ressource aus.
4. Im Abschnitt IPv6-Netzwerk der Seite wählen Sie den Schalter, um IPv6 für die Ressource zu deaktivieren.



SSL/TLS-Zertifikate in Amazon Lightsail

Amazon Lightsail verwendet SSL/TLS-Zertifikate, um benutzerdefinierte (registrierte) Domains zu validieren, die Sie mit Lightsail-Load Balancern, Content Delivery Network (CDN) -Distributionen (CDN) und Container-Services verwenden können. Nachdem ein validiertes Zertifikat an eine dieser Lightsail-Ressourcen angehängt wurde, wird der Datenverkehr, der über die Domain zu dieser Ressource geleitet wird, mit Hypertext Transfer Protocol Secure (HTTPS) verschlüsselt.

Sie können Transport Layer Security (TLS) -Zertifikate in Amazon Lightsail erstellen, um verschlüsselten Webdatenverkehr für benutzerdefinierte (registrierte) Domains zu aktivieren, die Sie

mit Ihren Lightsail-Load Balancern, Content Delivery Network-Distributionen und Container-Services verwenden möchten. TLS ist eine aktualisierte, sicherere Version von SSL (Secure Socket Layer). In der Lightsail-Dokumentation und -Konsole werden Sie sehen, dass wir es als SSL/TLS bezeichnen.

> **Note**
>
> Die Lightsail-Zertifikate, die Sie an Load Balancer, CDN-Distributionen und Containerdienste anhängen können, werden vom (ACM) -Dienst ausgestellt. AWS Certificate Manager Ab dem 11. Oktober 2022 wird jedes öffentliche Zertifikat, das Sie über Lightsail für Ihre Load Balancer, CDN-Distributionen und Containerdienste erhalten haben, von einer der mehreren Intermediate Certificate Authority (ICAs) oder untergeordneten Zertifizierungsstellen ausgestellt, die ACM verwaltet. Weitere Informationen finden Sie unter Amazon führt dynamische Zwischenzertifizierungsstellen ein im AWS-Sicherheitsblog.

Warum HTTPS verwenden?

Vor allem dient es der Sicherheit. HTTPS bietet zusätzliche Sicherheit, da es TLS zum Verschieben von Daten verwendet. Die HTTPS-Verschlüsselung ist vertraulich zwischen dem Webserver und dem Client-Browser, da sie die beiden einzigen Entitys darstellen, die den Datenverkehr entschlüsseln können. HTTPS-Verbindungen sind außerdem sicherer, da die Daten, die ein Client mit dem Server austauscht, von keiner anderen Partei geändert werden kann.

Außer den oben genannten Vorteilen für die Sicherheit sprechen noch andere Gründe für die Verwendung von HTTPS zusätzlich zu HTTP. Google begann im Jahr 2014 z. B., sichere Websites in den Suchergebnissen in der Rangfolge höher einzustufen. Mit anderen Worten, eine Website, die HTTPS verwendet, wird weiter oben in den Suchergebnissen angezeigt als eine Website, die nur HTTP verwendet (bei ansonsten identischen Merkmalen).

Weitere Informationen über HTTPS als Rangfolgesignal

Prozessübersicht

Das Verfahren zur Verwendung eines Lightsail-Zertifikats ist einfach. Es umfasst die folgenden Schritte:

1. Erstellen Sie Ihre Lightsail-Ressource, die ein Lightsail-Zertifikat verwenden kann, z. B. einen Load Balancer, eine CDN-Distribution oder einen Container-Service.

2. Erstellen Sie mit Lightsail ein Zertifikat für Ihre Domain.
3. Überprüfen Sie das Zertifikat, indem Sie dem DNS Ihrer Domäne einen Canonical-Name (CNAME)-Datensatz hinzufügen
4. Hängen Sie das validierte Zertifikat an Ihre Lightsail-Ressource an.
5. Ändern Sie den DNS Ihrer Domain, um den Verkehr an Ihre Lightsail-Ressource weiterzuleiten.

Nachdem ein validiertes Zertifikat an die Ressource angehängt wurde, wird der Datenverkehr, der über die Domäne an diese Ressource umgeleitet wird, mit Hypertext Transfer Protocol Secure (HTTPS) verschlüsselt.

Verwenden von SSL-/TLS-Zertifikaten in Verbindung mit Ihrer Verteilung oder Container-Service

HTTPS ist für Lightsail-Distributionen und Container-Services erforderlich. Wenn Sie eine dieser Ressourcen erstellen, ist HTTPS standardmäßig für die Standarddomäne der Ressource aktiviert (z. B. `https://123456abcdef.cloudfront.net/` für eine Verteilungen oder `https://container-service-1.123456abcdef.us-west-2.cs.amazonlightsail.com/` für einen Container-Service). Wenn Sie Ihren registrierten Domainnamen (z. B.`example.com`) mit Ihrem Vertriebs- oder Containerdienst verwenden möchten, müssen Sie ein Lightsail-SSL/TLS-Zertifikat erstellen, es mit Ihrem Domainnamen validieren und benutzerdefinierte Domains auf Ihrer Ressource aktivieren. Wenn Sie benutzerdefinierte Domänen in Ihrer Verteilung oder Ihrem Container-Service aktivieren, wird auch das validierte Zertifikat Ihrer Domäne an Ihre Ressource angehängt.

Folgen Sie diesen Links, um benutzerdefinierte Domänen und HTTPS in Ihrer Verteilung zu aktivieren.

- Erstellen von SSL-/TLS-Zertifikaten für Ihre Verteilung
- Validieren von SSL-/TLS-Zertifikaten für Ihre Verteilung
- Anzeigen von SSL-/TLS-Zertifikaten für Ihre Verteilung

- Aktivieren benutzerdefinierter Domains für Ihre Verteilung
- Verweisen Sie Ihre Domain auf eine Verteilung

Weitere Informationen zu Verteilungen finden Sie unter Netzwerkverteilungen für die Bereitstellung von Inhalten.

Folgen Sie diesen Links, um benutzerdefinierte Domänen und HTTPS in Ihrem Container-Service zu aktivieren.

- Erstellen Sie ein SSL-/TLS-Zertifikat für Ihre Container-Services
- Validieren Sie ein SSL-/TLS-Zertifikat für Ihre Container-Services
- Aktivieren und verwalten Sie benutzerdefinierte Domains

Weitere Informationen zu Container-Services finden Sie unter Container-Services.

Verwenden von SSL-/TLS-Zertifikaten mit Ihrem Load Balancer

Wenn Sie einen Lightsail-Load Balancer erstellen, ist Port 80 standardmäßig für die Verarbeitung von regulärem HTTP-Verkehr geöffnet. Um HTTPS-Datenverkehr über Port 443 zu aktivieren, müssen Sie ein SSL/TLS-Zertifikat erstellen, es mit Ihrem Domänennamen validieren und es an Ihren Load Balancer anhängen.

Sie können bis zu zwei SSL-/TLS-Zertifikate pro Load Balancer erstellen. Pro Load Balancer kann jeweils nur ein Zertifikat verwendet werden. Wenn Sie ein gültiges, aktives Zertifikat von Ihrem Load Balancer löschen, können Sie für die jeweilige Domäne keinen verschlüsselten HTTPS-Datenverkehr mit Ihrem Load Balancer verarbeiten, bis Sie ein anderes gültiges Zertifikat anfügen.

Ersten Schritte zu der Aktivierung von HTTPS auf Ihrem Load Balancer finden Sie in den folgenden Links.

- Erstellen eines Load Balancers und Anfügen von Instances
- Erstellen eines SSL-/TLS-Zertifikats
- Überprüfen des Domäneneigentümers
- Anfügen des überprüften Zertifikats zum Aktivieren von HTTPS

Weitere Informationen über Load Balancer finden Sie unter Load Balancer.

SSL-/TLS-Zertifikate für Lightsail-Container-Services

Sie können Amazon Lightsail-TLS-/SSL-Zertifikate für Ihren Lightsail-Container-Service erstellen. Wenn Sie ein Zertifikat erstellen, geben Sie den primären und alternativen Domänennamen für das Zertifikat an. Wenn Sie benutzerdefinierte Domänen für Ihren Container-Service aktivieren und das Zertifikat auswählen, können Sie bis zu vier Domänen aus dem Zertifikat auswählen, die als benutzerdefinierte Domänen Ihres Container-Services hinzugefügt werden. Nachdem Sie die DNS-Akte Ihrer Domänen aktualisiert haben, um den Datenverkehr auf Ihren Container-Service zu leiten, akzeptiert Ihr Dienst den Datenverkehr und stellt Ihre Inhalte mithilfe von HTTPS bereit. Es gibt ein Kontingent für die Anzahl der Zertifikate, die Sie erstellen können. Weitere Informationen finden Sie unter Lightsail-Servicekontingente.

Weitere Informationen zu SSL-/TLS-Zertifikaten finden Sie unter Container-Service-Zertifikate.

Voraussetzungen

Bevor Sie beginnen, müssen Sie einen Lightsail-Container-Services erstellen. Weitere Informationen finden Sie unter Erstellen von Container-Services und Container-Services.

Erstellen Sie ein SSL-/TLS-Zertifikat für Ihre Container-Services

Vervollständigen Sie das folgende Verfahren, um ein SSL-/TLS-Zertifikat für Ihren Container-Service zu erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen des Container-Servicess aus, für den Sie ein Zertifikat erstellen möchten.
4. Wählen Sie die Registerkarte Benutzerdefinierte Domänen auf der Verwaltungsseite Ihres Container-Servicess aus.
5. Scrollen Sie auf der Seite nach unten zum Abschnitt Attached certificates (Angefügte Zertifikate).

   Alle Ihre Zertifikate sind auf der Seite unter dem Abschnitt „Attached certificates“ (Angefügte Zertifikate) aufgeführt – einschließlich Zertifikaten, die für andere Lightsail-Ressourcen erstellt wurden, und Zertifikaten, die verwendet und nicht verwendet werden.
6. Wählen Sie Create certificate (Zertifikat erstellen).
7. Geben Sie in das Textfeld Certificate name (Zertifikatname) einen eindeutigen Namen ein, um Ihr Zertifikat zu identifizieren. Klicken Sie nun auf Continue (Weiter).

8. Geben Sie den primären Domänennamen (z. B. `example.com`), den Sie mit dem Zertifikat verwenden möchten, im Textfeld Specify up to 10 domains or subdomains (Bis zu 10 Domänen oder Unterdomänen angeben) ein.
9. (Optional) Geben Sie einen anderen Domänennamen (z. B. www.beispiel.com) in das Feld Specify up to 10 domains or subdomains (Bis zu 10 Domänen oder Unterdomänen angeben) ein.

   Sie können dem Zertifikat bis zu neun alternative Domänen hinzufügen. Sie können bis zu vier Domänen Ihres Zertifikats mit Ihrem Container-Service verwenden, nachdem Sie benutzerdefinierte Domänen aktiviert und das Zertifikat für Ihren Dienst ausgewählt haben.
10. Wählen Sie Create certificate (Zertifikat erstellen).

    Ihre Zertifikatsanforderung wird gesendet und der Status Ihres neuen Zertifikats wird in Attempting to validate your certificate (Es wird versucht, Ihr Zertifikat zu validieren) geändert. Während dieser Zeit versucht Lightsail, den Validierungsdatensatz des Zertifikats zum DNS der primären Domäne hinzuzufügen. Nach einiger Zeit ändert sich der Status in Valid (Gültig).

    Wenn die automatische Validierung fehlschlägt, müssen Sie das Zertifikat mit Ihren Domänen validieren, bevor Sie es mit Ihrem Container-Service verwenden können. Weitere Informationen finden Sie unter Validierung von SSL-/TLS-Zertifikaten.

Themen

Validieren von SSL-/TLS-Zertifikaten für Lightsail-Container-Services

Ein Amazon Lightsail-SSL-/TLS-Zertifikat muss validiert werden, nachdem Sie es erstellt haben und bevor Sie es mit Ihrem Lightsail-Container-Service benutzen können. Nachdem Ihre Zertifikatsanforderung gesendet wurde, wird der Status Ihres neuen Zertifikats in Attempting to validate your certificate (Es wird versucht, Ihr Zertifikat zu validieren) geändert. Während dieser Zeit versucht Lightsail, den Validierungsdatensatz des Zertifikats zum DNS der Domänennamen hinzuzufügen, die Sie für das Zertifikat angegeben haben. Nach einer Weile ändert sich der Status in Valid (Gültig) oder in Validation timed out (Zeitüberschreitung für die Validierung).

Wenn die automatische Validierung scheitert, müssen Sie überprüfen, ob Sie Kontrolle über alle Domänennamen haben, die Sie für das Zertifikat angegeben haben, als Sie es erstellt haben. Dazu fügen Sie kanonische Namenseinträge (CNAME) zur DNS-Zone jeder der im Zertifikat angegebenen

Domänen hinzu. Die Datensätze, die Sie hinzufügen müssen, werden im Abschnitt mit den Validation details (Validierungsdetails) des Zertifikats aufgelistet.

In diesem Leitfaden stellen wir Ihnen das Verfahren zur manuellen Validierung Ihres Zertifikats mit einer Lightsail-DNS-Zone vor. Das Verfahren, um Ihr Zertifikat mithilfe eines anderen DNS-Hostinganbieters wie Domain.com oder GoDaddy zu validieren, kann ähnlich sein. Weitere Informationen über Lightsail-DNS-Zonen finden Sie unter DNS.

Weitere Informationen zu SSL-/TLS-Zertifikaten finden Sie unter SSL-/TLS-Zertifikate.

Voraussetzung

Bevor Sie beginnen, müssen Sie ein SSL-/TLS-Zertifikat für Ihren Container-Service erstellen. Weitere Informationen finden Sie unter Erstellen von SSL-/TLS-Zertifikaten für Ihre Container-Services.

Holen Sie sich die CNAME-Datensatzwerte, um Ihr Zertifikat zu validieren

Führen Sie das folgende Verfahren aus, um die CNAME-Einträge abzurufen, die Sie Ihren Domänen hinzufügen müssen, um das Zertifikat zu validieren.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen des Container-Servicess aus, für den Sie ein Zertifikat erstellen möchten.
4. Wählen Sie die Registerkarte Benutzerdefinierte Domänen auf der Verwaltungsseite Ihres Container-Servicess aus.
5. Scrollen Sie auf der Seite nach unten zum Abschnitt Attached certificates (Angefügte Zertifikate).

   Alle Ihre Zertifikate sind auf der Seite unter dem Abschnitt Attached certificates (Angefügte Zertifikate) aufgelistet – einschließlich der Zertifikate, die für andere Lightsail-Ressourcen erstellt wurden, und der Zertifikate, die noch validiert werden müssen.
6. Suchen Sie das Zertifikat, das Sie validieren möchten, erweitern Sie Validation details (Validierungsdetails) und notieren Sie sich Name und Wert der CNAME-Datensätze, die Sie für jede aufgelistete Domäne hinzufügen müssen.

   Sie müssen diese Datensätze genau wie aufgelistet hinzufügen. Es wird empfohlen, diese Werte zu kopieren und in eine Textdatei einzufügen, auf die Sie später verweisen können. Weitere

Informationen finden Sie unter den folgenden Abschnitten Hinzufügen der CNAME-Akten zur DNS-Zone Ihrer Domäne in diesem Leitfaden.

Hinzufügen von CNAME-Datensätzen zu den DNS-Einstellungen Ihrer Domäne

Führen Sie das folgende Verfahren aus, um zur DNS-Zone Ihrer Domain CNAME-Datensätze hinzuzufügen.

1. Wählen Sie auf der Lightsail-Startseite die Registerkarte Domains & DNS (Domänen und DNS).
2. Unter dem Abschnitt DNS-Zonen der Seite wählen Sie den Domänennamen aus, der Sie die CNAME-Datensätze hinzufügen möchten, um das Zertifikat zu validieren.
3. Wählen Sie die Registerkarte DNS records (DNS-Datensätze) aus.
4. Wählen Sie auf der Seite zur Verwaltung der DNS-Datensätze die Option Add record (Datensatz hinzufügen) aus.
5. Wählen Sie CNAME im Dropdown-Menü Record type (Datensatztyp) aus.
6. Geben Sie im Textfeld Record name (Datensatzname) den Wert Name des CNAME-Datensatzes ein, den Sie von Ihrem Zertifikat erhalten haben.

   Die Lightsail-Konsole füllt den oberen Teil Ihrer Domäne vorab aus. Wenn Sie beispielsweise das `www.example.com`-Subdomain hinzufügen möchten, dann müssen Sie im Textfeld nur `www` eingeben und Lightsail fügt das `.example.com`-Teil für Sie hinzu, wenn Sie den Datensatz speichern.
7. Geben Sie im Textfeld Route traffic to (Datenverkehr weiterleiten an) den Value (Wert) des CNAME-Datensatzes ein, den Sie von Ihrem Zertifikat erhalten haben.
8. Bestätigen Sie, dass die eingegebenen Werte genau so sind, wie sie in dem Zertifikat aufgeführt sind, das Sie validieren möchten.
9. Wählen Sie das Symbol „Speichern“, um die Akte in Ihrer DNS-Zone zu speichern.

   Wiederholen Sie diese Schritte, um zusätzliche CNAME-Einträge für Domänen in Ihrem Zertifikat hinzuzufügen, die validiert werden müssen. Warten Sie einige Zeit, damit sich Änderungen über das DNS im Internet ausbreiten. Nach einigen Minuten sollten Sie sehen, ob der Status Ihres Zertifikat in Gültig ändert. Weitere Informationen finden Sie im Abschnitt Anzeigen des Status Ihres Zertifikats in diesem Leitfaden.

Anzeigen des Status Ihres Zertifikats

Führen Sie die folgenden Schritte aus, um den Status Ihres SSL-/TLS-Zertifikats anzuzeigen.

1. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
2. Wählen Sie den Namen des Container-Servicess aus, für den Sie ein Zertifikat erstellen möchten.
3. Wählen Sie die Registerkarte Benutzerdefinierte Domänen auf der Verwaltungsseite Ihres Container-Servicess aus.
4. Scrollen Sie auf der Seite nach unten zum Abschnitt Attached certificates (Angefügte Zertifikate).

   Alle Ihre Zertifikate sind unter dem Abschnitt Attached certificates (Angefügte Zertifikate) der Seite aufgelistet – einschließlich der Zertifikate mit Status Pending validation (Ausstehende Validierung) und Valid (Gültig).

   > **Note**
   >
   > Wenn Sie die Seite Custom domains (Benutzerdefinierte Domänen) während der Überprüfung Ihrer Zertifikate geöffnet haben, müssen Sie möglicherweise aktualisieren, um den aktualisierten Status Ihrer Zertifikate anzuzeigen.

   A Gültig-Status bestätigt, dass Sie Ihr Zertifikat erfolgreich mit den CNAME-Datensätzen validiert haben, die Sie Ihren Domänen hinzugefügt haben. Wählen Sie Details, um wichtige Datumsangaben, Verschlüsselungsdetails, Identifikations- und Validierungsdatensätze Ihres Zertifikats anzuzeigen. Ihre Zertifikate sind ab dem Datum, an dem Sie sie validiert haben, 13 Monate gültig. Lightsail versucht, sie automatisch neu zu validieren. Löschen Sie die CNAME-Einträge, die Sie Ihrer Domäne hinzugefügt haben, nicht, da sie erforderlich sind, wenn Ihr Zertifikat am angegebenen Datum Gültig bis erneut validiert wird.

   Nachdem Sie Ihr SSL/TLS-Zertifikat validiert haben, sollten Sie benutzerdefinierte Domänen für Ihren Container-Service aktivieren, um die Domänennamen Ihres Zertifikats in Ihrem Dienst zu verwenden. Weitere Informationen finden Sie unter Aktivieren und Verwalten benutzerdefinierter Domains für Ihre Container-Services.

Anzeigen von SSL-/TLS-Zertifikaten für Lightsail-Container-Services

Sie können Amazon Lightsail-TLS-/SSL-Zertifikate für Ihren Lightsail-Container-Service erstellen. Dazu greifen Sie auf die Verwaltungsseite eines beliebigen Container-Service in der Lightsail-Konsole zu.

Weitere Informationen zu SSL-/TLS-Zertifikaten finden Sie unter SSL-/TLS-Zertifikate.

Voraussetzungen

Bevor Sie beginnen, müssen Sie einen Lightsail-Container-Services erstellen. Weitere Informationen finden Sie unter Erstellen von Amazon Lightsail-Container-Services und Container-Services.

Außerdem sollten Sie ein SSL-/TLS-Zertifikat für Ihren Container-Service erstellt und validiert haben. Weitere Informationen finden Sie unter Erstellen von SSL-/TLS-Zertifikaten für Container-Services.

Anzeigen von SSL-/TLS-Zertifikaten für Container-Services

Vervollständigen Sie das folgende Verfahren, um ein SSL-/TLS-Zertifikat für Ihren Container-Service zu erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen eines Container-Servicess.

   Sie können alle Zertifikate unabhängig vom ausgewählten Container-Service anzeigen.
4. Wählen Sie die Registerkarte Benutzerdefinierte Domänen auf der Verwaltungsseite Ihres Container-Servicess aus.
5. Scrollen Sie auf der Seite nach unten zum Abschnitt Attached certificates (Angefügte Zertifikate).

   Alle Ihre Zertifikate sind unter dem Abschnitt Attached certificates (Angefügte Zertifikate) der Seite aufgelistet. Wählen Sie Details, um wichtige Datumsangaben, Verschlüsselungsdetails, Identifikation und Domänen Ihres Zertifikats anzuzeigen. Wählen Sie Validation details (Validierungsdetails), um die Validierungsdatensätze Ihres Zertifikats einzusehen. Ihre Zertifikate sind ab dem Datum, an dem Sie sie validiert haben, 13 Monate gültig.Lightsail versucht, sie automatisch neu zu validieren. Löschen Sie die CNAME-Einträge, die Sie Ihrer Domäne hinzugefügt haben, nicht, da sie erforderlich sind, wenn Ihr Zertifikat am angegebenen Datum Gültig bis erneut validiert wird.

Nachdem Sie ein gültiges SSL-/TLS-Zertifikat für den Container-Service verwendet haben, sollten Sie benutzerdefinierte Domänen aktivieren, damit Sie die Domänennamen des Zertifikats in Ihrem Dienst verwenden können. Weitere Informationen finden Sie unter Aktivieren und verwalten benutzerdefinierter Domains.

SSL-/TLS-Zertifikate für Lightsail-Vertrieb

Sie können Amazon Lightsail TLS/SSL-Zertifikate für Ihre Lightsail-Distributionen erstellen. Wenn Sie ein Zertifikat erstellen, geben Sie den primären und alternativen Domänennamen für das Zertifikat an. Wenn Sie benutzerdefinierte Domänen für Ihre Verteilung aktivieren und das Zertifikat auswählen, werden diese Domänen als benutzerdefinierte Domänen Ihrer Verteilung hinzugefügt. Nachdem Sie den DNS-Akte Ihrer Domänen aktualisiert haben, um auf Ihre Verteilung zu verweisen, akzeptiert Ihre Verteilung den Datenverkehr und stellt Ihre Inhalte mithilfe von HTTPS bereit. Es gibt ein Kontingent für Anzahl der Zertifikate, die Sie erstellen können. Weitere Informationen finden Sie unter Lightsail-Service-Quotas.

Weitere Informationen zu SSL-/TLS-Zertifikaten finden Sie unter SSL-/TLS-Zertifikate.

> **Important**
>
> Die Domainnamen, die Sie bei der Erstellung eines SSL/TLS-Zertifikats für Ihre Distribution angeben, dürfen nicht von einer anderen Distribution für alle Amazon Web Services (AWS) - Konten verwendet werden, einschließlich Verteilungen auf dem Amazon-Service. CloudFront Sie können das Zertifikat für die Domänen erstellen, aber Sie können das Zertifikat nicht mit Ihrer Verteilung verwenden.

Voraussetzung

Bevor Sie beginnen, müssen Sie eine Lightsail-Distribution erstellen. Weitere Informationen finden Sie unter Erstellen einer Verteilung und Netzwerkverteilungen für die Bereitstellung von Inhalten.

Erstellen eines SSL-/TLS-Zertifikates für Ihre Verteilung

Vervollständigen Sie das folgende Verfahren, um ein SSL-/TLS-Zertifikat für die Verteilung zu erstellen.

1. Melden Sie sich bei der Lightsail-Konsole an.

2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Networking (Netzwerk).
3. Wählen Sie den Namen der Verteilung aus, für die Sie ein Zertifikat erstellen möchten.
4. Wählen Sie die Registerkarte Benutzerdefinierte Domänenauf der Verwaltungsseite Ihrer Verteilung aus.
5. Scrollen Sie auf der Seite nach unten zum Abschnitt Attached certificates (Angefügte Zertifikate).

   Alle Ihre Verteilungszertifikate sind auf der Seite unter dem Abschnitt Attached certificates (Angefügte Zertifikate) aufgeführt – einschließlich Zertifikaten, die für andere Verteilungen erstellt wurden, und Zertifikaten, die verwendet und nicht verwendet werden.
6. Wählen Sie Create certificate (Zertifikat erstellen).
7. Geben Sie in das Textfeld Certificate name (Zertifikatname) einen eindeutigen Namen ein, um Ihr Zertifikat zu identifizieren. Klicken Sie nun auf Continue (Weiter).
8. Geben Sie den primären Domänennamen (z. B. `example.com`), den Sie mit dem Zertifikat verwenden möchten, im Textfeld Specify up to 10 domains or subdomains (Bis zu 10 Domänen oder Unterdomänen angeben) ein.
9. (Optional) Geben Sie alternative Domänenamen (z. B. `www.example.com`) in die verbleibenden Felder Specify up to 10 domains or subdomains (Bis zu 10 Domänen oder Unterdomänen angeben) ein.

   Sie können Ihrem Zertifikat bis zu neun alternative Domänen hinzufügen. Sie werden alle Domänen Ihres Zertifikats mit Ihrer Verteilung verwenden können, nachdem Sie benutzerdefinierte Domänen aktiviert und das Zertifikat für Ihre Verteilung ausgewählt haben.
10. Wählen Sie Erstellen.

    Ihre Zertifikatsanforderung wird gesendet und der Status Ihres neuen Zertifikats wird in Attempting to validate your certificate (Es wird versucht, Ihr Zertifikat zu validieren) geändert. Während dieser Zeit versucht Lightsail, den Bestätigungseintrag des Zertifikats zum DNS der primären Domain hinzuzufügen. Nach einiger Zeit ändert sich der Status in Valid (Gültig).

    Wenn die automatische Validierung fehlschlägt, müssen Sie das Zertifikat mit Ihren Domänen validieren, bevor Sie es mit Ihrer Verteilung verwenden können. Weitere Informationen finden Sie unter Validierung von SSL-/TLS-Zertifikaten für Ihre Verteilung.

Themen

- SSL/TLS-Zertifikate für Ihre Lightsail-Distribution anzeigen

- Validieren von SSL-/TLS-Zertifikaten für Ihre Lightsail-Verteilung
- Konfigurieren Sie die Mindestversion des TLS-Protokolls für Ihr Lightsail-Vertriebszertifikat
- Löschen eines SSL-/TLS-Zertifikats für Ihre Lightsail-Verteilung

SSL/TLS-Zertifikate für Ihre Lightsail-Distribution anzeigen

Sie können die Amazon Lightsail SSL/TLS-Zertifikate einsehen, die Sie für Ihre Lightsail-Distributionen erstellt haben. Sie tun dies, indem Sie in der Lightsail-Konsole auf die Verwaltungsseite einer beliebigen Distribution zugreifen.

Weitere Informationen zu SSL-/TLS-Zertifikaten finden Sie unter SSL-/TLS-Zertifikate.

Voraussetzungen

Bevor Sie beginnen, müssen Sie eine Lightsail-Distribution erstellen. Weitere Informationen finden Sie unter Erstellen einer Verteilung und Netzwerkverteilungen für die Bereitstellung von Inhalten.

Sie sollten auch ein SSL-/TLS-Zertifikat für die Verteilung erstellt haben. Weitere Informationen finden Sie unter Erstellen von SSL-/TLS-Zertifikaten für Ihre Verteilung.

Anzeigen von SSL-/TLS-Zertifikaten für Ihre Verteilung

Vervollständigen Sie das folgende Verfahren, um ein SSL-/TLS-Zertifikat für die Verteilung zu löschen.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Networking (Netzwerk).
3. Wählen Sie den Namen einer Verteilung aus.

   Sie können alle Ihre Zertifikate unabhängig von der ausgewählten Verteilung anzeigen.
4. Wählen Sie die Registerkarte Benutzerdefinierte Domänen auf der Verwaltungsseite Ihrer Verteilung aus.
5. Scrollen Sie auf der Seite nach unten zum Abschnitt Attached certificates (Angefügte Zertifikate).

   Alle Ihre Verteilungszertifikate sind unter dem Abschnitt Attached certificates (Angefügte Zertifikate) der Seite aufgelistet. Erweitern Sie Validation details (Validierungsdetails), um wichtige Datumsangaben, Verschlüsselungsdetails, Identifikations- und Validierungsdatensätze Ihres Zertifikats anzuzeigen. Ihre Zertifikate sind ab dem Datum, an dem Sie sie validiert haben,

13 Monate gültig. versucht, sie automatisch neu zu validieren. Löschen Sie die CNAME-Einträge, die Sie Ihrer Domäne hinzugefügt haben, nicht, da sie erforderlich sind, wenn Ihr Zertifikat am angegebenen Datum Gültig bis erneut validiert wird.

Nachdem Sie ein gültiges SSL-/TLS-Zertifikat für den Container-Service verwendet haben, sollten Sie benutzerdefinierte Domänen aktivieren, damit Sie die Domänennamen des Zertifikats in Ihrem Dienst verwenden können. Weitere Informationen finden Sie unter Aktivieren benutzerdefinierter Domains für Ihre Verteilung.

Validieren von SSL-/TLS-Zertifikaten für Ihre Lightsail-Verteilung

Ein Amazon Lightsail-SSL-/TLS-Zertifikat muss validiert werden, nachdem Sie es erstellt haben und bevor Sie es mit Ihrer Lightsail-Verteilung benutzen können. Nachdem Ihre Zertifikatsanforderung gesendet wurde, wird der Status Ihres neuen Zertifikats in Attempting to validate your certificate (Es wird versucht, Ihr Zertifikat zu validieren) geändert. Während dieser Zeit versucht Lightsail, den Validierungsdatensatz des Zertifikats zum DNS der Domänennamen hinzuzufügen, die Sie für das Zertifikat angegeben haben. Nach einer Weile ändert sich der Status in Valid (Gültig) oder in Validation timed out (Zeitüberschreitung für die Validierung).

Wenn die automatische Validierung scheitert, müssen Sie überprüfen, ob Sie Kontrolle über alle Domänennamen haben, die Sie für das Zertifikat angegeben haben, als Sie es erstellt haben. Dazu fügen Sie kanonische Namenseinträge (CNAME) zur DNS-Zone jeder der im Zertifikat angegebenen Domänen hinzu. Die Datensätze, die Sie hinzufügen müssen, werden im Abschnitt mit den Validation details (Validierungsdetails) des Zertifikats aufgelistet.

In diesem Leitfaden stellen wir Ihnen das Verfahren zur manuellen Validierung Ihres Zertifikats mit einer Lightsail-DNS-Zone vor. Das Verfahren, um Ihr Zertifikat mithilfe eines anderen DNS-Hostinganbieters wie Domain.com oder GoDaddy zu validieren, kann ähnlich sein. Weitere Informationen über Lightsail-DNS-Zonen finden Sie unter DNS.

Weitere Informationen zu SSL-/TLS-Zertifikaten finden Sie unter SSL-/TLS-Zertifikate.

Inhalt

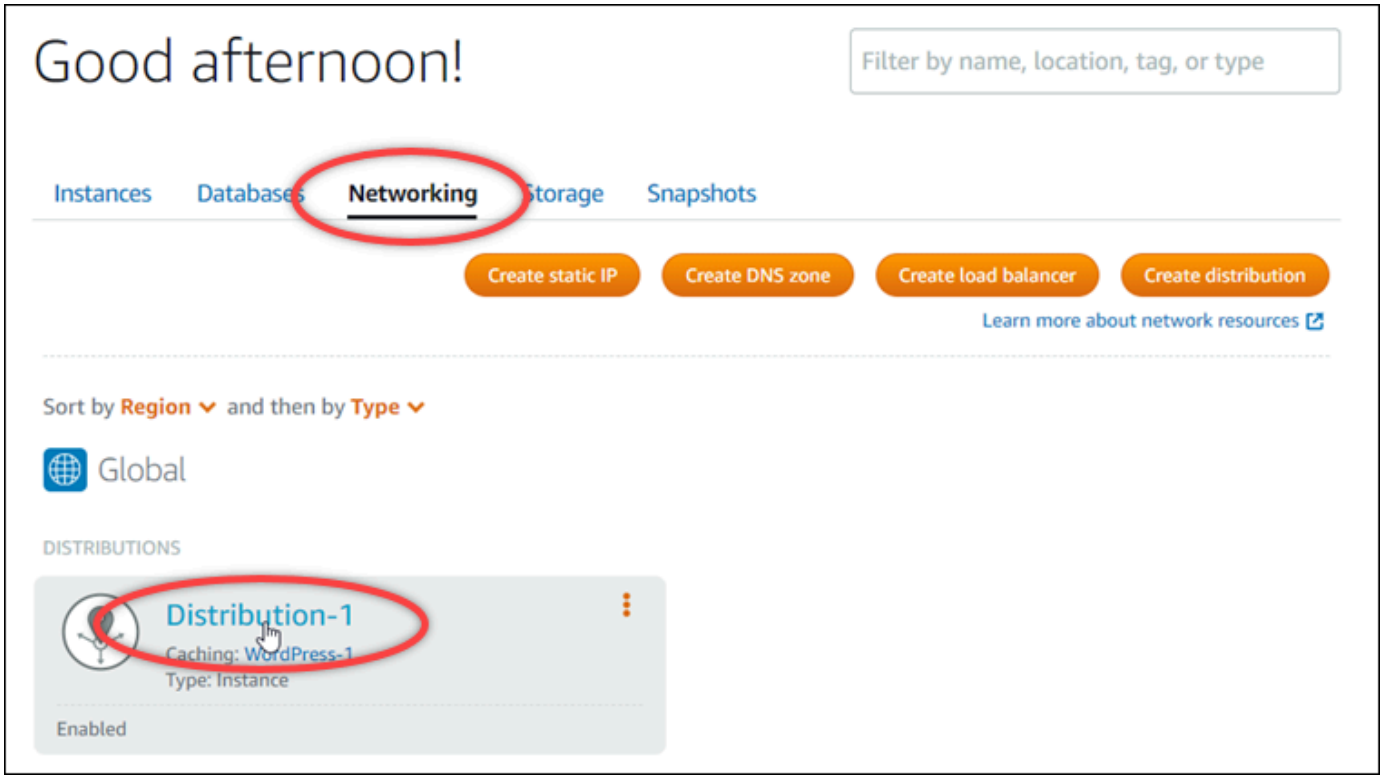
Voraussetzung

Bevor Sie beginnen, müssen Sie ein SSL-/TLS-Zertifikat für Ihre Verteilung erstellen. Weitere Informationen finden Sie unter Erstellen von SSL-/TLS-Zertifikaten für Ihre Verteilung.

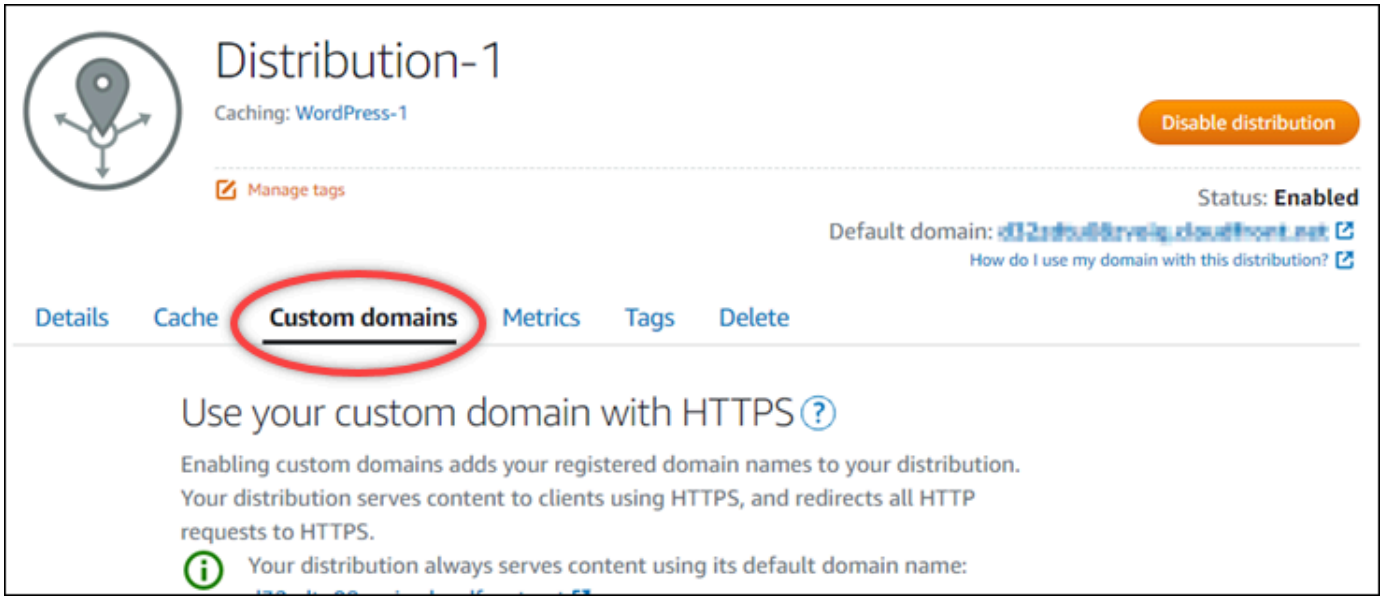
Holen Sie sich die CNAME-Datensatzwerte, um Ihr Zertifikat zu validieren

Führen Sie das folgende Verfahren aus, um die CNAME-Einträge abzurufen, die Sie Ihren Domänen hinzufügen müssen, um das Zertifikat zu validieren.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen der Verteilung, für die die CNAME-Datensatzwerte eines Zertifikats abgerufen werden sollen.



4. Wählen Sie die Registerkarte Benutzerdefinierte Domänen auf der Verwaltungsseite Ihrer Verteilung aus.



5. Scrollen Sie auf der Seite nach unten zum Abschnitt Attached certificates (Angefügte Zertifikate).

   Alle Ihre Verteilungszertifikate sind auf der Seite unter dem Abschnitt Attached certificates (Angefügte Zertifikate) aufgelistet – einschließlich der Zertifikate, die für andere Lightsail-Ressourcen erstellt wurden, und der Zertifikate, die noch validiert werden müssen.

6. Suchen Sie das Zertifikat, das Sie validieren möchten, erweitern Sie Validation details (Validierungsdetails) und notieren Sie sich Name und Wert der CNAME-Datensätze, die Sie für jede aufgelistete Domäne hinzufügen müssen.

   Sie müssen diese Datensätze genau wie aufgelistet hinzufügen. Es wird empfohlen, diese Werte zu kopieren und in eine Textdatei einzufügen, auf die Sie später verweisen können. Weitere Informationen finden Sie unter den folgenden Abschnitten Hinzufügen der CNAME-Akten zur DNS-Zone Ihrer Domäne in diesem Leitfaden.

Hinzufügen von CNAME-Datensätzen zu den DNS-Einstellungen Ihrer Domäne

Führen Sie das folgende Verfahren aus, um zur DNS-Zone Ihrer Domain CNAME-Datensätze hinzuzufügen.

1. Wählen Sie auf der Lightsail-Startseite die Registerkarte Domains & DNS (Domänen und DNS).
2. Unter dem Abschnitt DNS-Zonen der Seite wählen Sie den Domänennamen aus, der Sie die CNAME-Datensätze hinzufügen möchten, um das Zertifikat zu validieren.
3. Wählen Sie die Registerkarte DNS records (DNS-Datensätze) aus.

4. Wählen Sie auf der Seite zur Verwaltung der DNS-Datensätze die Option Add record (Datensatz hinzufügen) aus.
5. Wählen Sie CNAME im Dropdown-Menü Record type (Datensatztyp) aus.
6. Geben Sie im Textfeld Record name (Datensatzname) den Wert Name des CNAME-Datensatzes ein, den Sie von Ihrem Zertifikat erhalten haben.

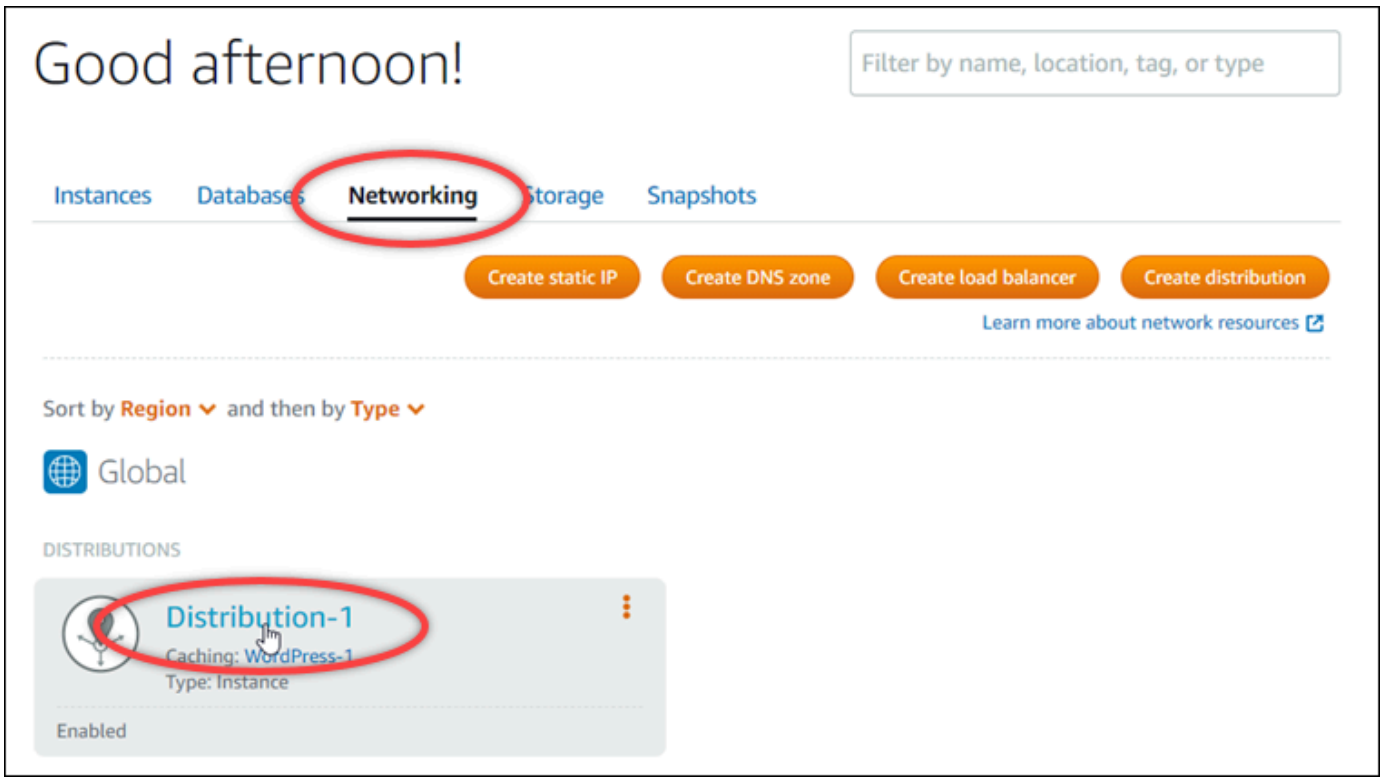
   Die Lightsail-Konsole füllt den oberen Teil Ihrer Domäne vorab aus. Wenn Sie beispielsweise das `www.example.com`-Subdomain hinzufügen möchten, dann müssen Sie im Textfeld nur `www` eingeben und Lightsail fügt das `.example.com`-Teil für Sie hinzu, wenn Sie den Datensatz speichern.
7. Geben Sie im Textfeld Route traffic to (Datenverkehr weiterleiten an) den Value (Wert) des CNAME-Datensatzes ein, den Sie von Ihrem Zertifikat erhalten haben.
8. Bestätigen Sie, dass die eingegebenen Werte genau so sind, wie sie in dem Zertifikat aufgeführt sind, das Sie validieren möchten.
9. Wählen Sie das Symbol „Speichern“, um die Akte in Ihrer DNS-Zone zu speichern.

   Wiederholen Sie diese Schritte, um zusätzliche CNAME-Einträge für Domänen in Ihrem Zertifikat hinzuzufügen, die validiert werden müssen. Warten Sie einige Zeit, damit sich Änderungen über das DNS im Internet ausbreiten. Nach einigen Minuten sollten Sie sehen, ob der Status Ihres Verteilungszertifikats in Gültig ändert. Weitere Informationen finden Sie im Abschnitt Anzeigen des Status Ihres Verteilungszertifikats in diesem Leitfaden.

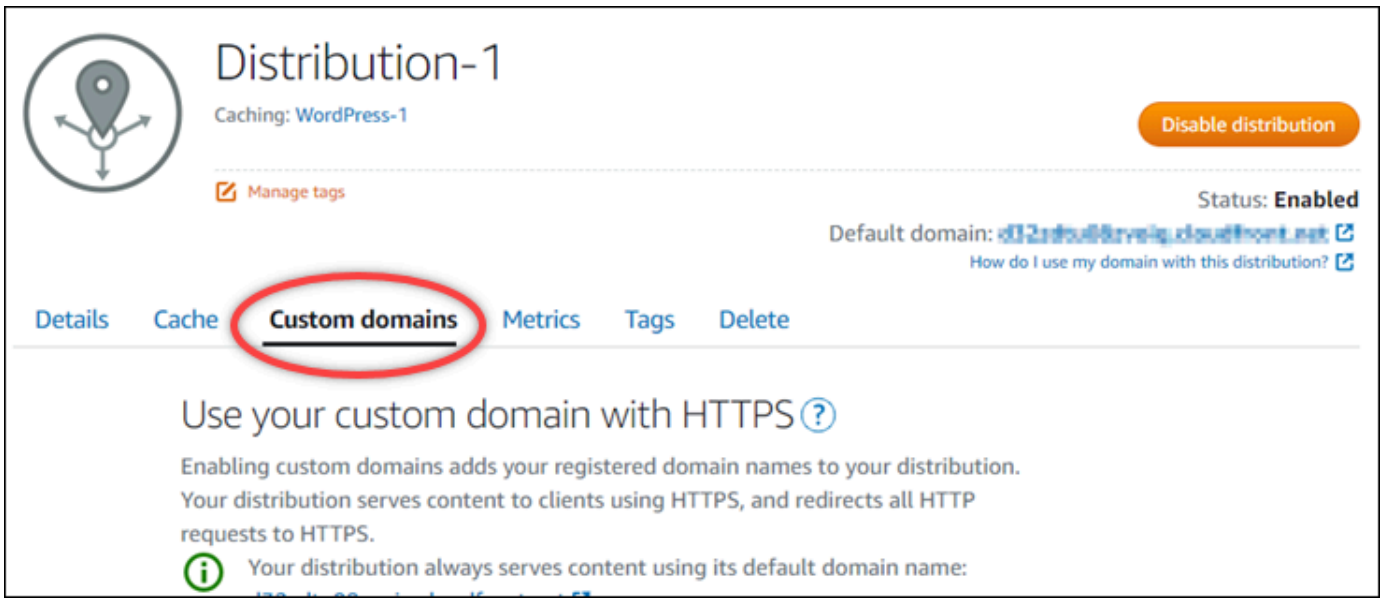
Anzeigen des Status Ihres Verteilungszertifikats

Vervollständigen Sie das folgende Verfahren, um ein SSL-/TLS-Zertifikat für die Verteilung zu löschen.

1. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
2. Wählen Sie den Namen der Verteilung aus, für die Sie den Status eines Zertifikats anzeigen möchten.

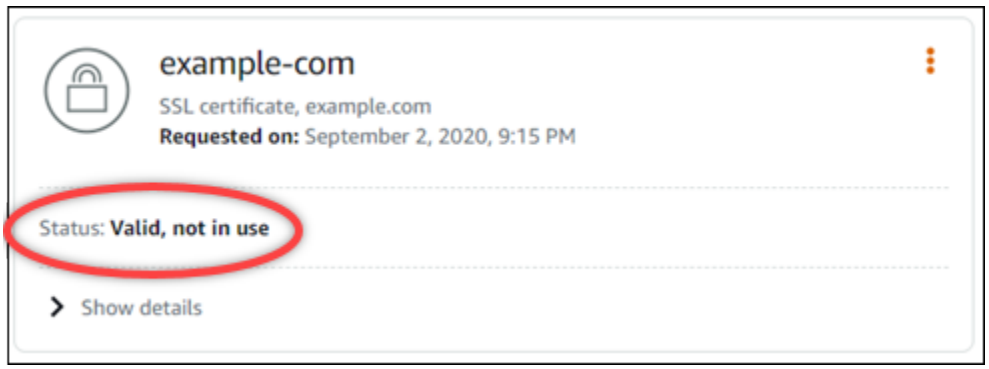


3. Wählen Sie die Registerkarte Benutzerdefinierte Domänen auf der Verwaltungsseite Ihrer Verteilung aus.



4. Scrollen Sie auf der Seite nach unten zum Abschnitt Attached certificates (Angefügte Zertifikate).

   Alle Ihre Verteilungszertifikate sind unter dem Abschnitt Attached certificates (Angefügte Zertifikate) der Seite aufgelistet – einschließlich der Zertifikate mit Status Pending validation (Ausstehende Validierung) und Valid (Gültig).



A Gültig-Status bestätigt, dass Sie Ihr Zertifikat erfolgreich mit den CNAME-Datensätzen validiert haben, die Sie Ihren Domänen hinzugefügt haben. Wählen Sie Details, um wichtige Datumsangaben, Verschlüsselungsdetails, Identifikations- und Validierungsdatensätze Ihres Zertifikats anzuzeigen. Ihre Zertifikate sind ab dem Datum, an dem Sie sie validiert haben, 13 Monate gültig. Lightsail versucht, sie automatisch neu zu validieren. Löschen Sie die CNAME-Einträge, die Sie Ihrer Domäne hinzugefügt haben, nicht, da sie erforderlich sind, wenn Ihr Zertifikat am angegebenen Datum Gültig bis erneut validiert wird.

Nachdem Sie Ihr SSL/TLS-Zertifikat validiert haben, sollten Sie benutzerdefinierte Domänen für Ihre Verteilung aktivieren, um die Domänennamen Ihres Zertifikats in Ihrer Verteilung zu verwenden. Weitere Informationen finden Sie unter Aktivieren benutzerdefinierter Domains für Ihre Verteilung.

Konfigurieren Sie die Mindestversion des TLS-Protokolls für Ihr Lightsail-Vertriebszertifikat

Amazon Lightsail verwendet SSL/TLS-Zertifikate, um benutzerdefinierte (registrierte) Domains zu validieren, die Sie mit Ihrer Lightsail-Distribution verwenden können. Dieses Handbuch enthält Informationen zu den minimalen TLS-Protokollversionen (Protokollversionen), die Sie für Ihr SSL/TLS-Zertifikat konfigurieren können. Weitere Informationen zu SSL-/TLS-Zertifikaten finden Sie unter SSL-/TLS-Zertifikate in Lightsail. Ein Viewer ist eine Anwendung, die HTTP-Anfragen an die Edge-Standorte sendet, die mit Ihrer Lightsail-Distribution verknüpft sind. Weitere Informationen zu Distributionen finden Sie unter Content Delivery Network-Distributionen in Lightsail.

Die `TLSv1.2_2021` Protokollversion wird standardmäßig konfiguriert, wenn Sie benutzerdefinierte Domänen für eine Verteilung aktivieren. Sie können eine andere Protokollversion konfigurieren, wie später in diesem Handbuch beschrieben. Lightsail-Distributionen unterstützen keine benutzerdefinierten TLS-Protokollversionen.

Unterstützte Protokolle

Lightsail-Distributionen können mit den folgenden TLS-Protokollen konfiguriert werden:

- (Empfohlen) TLSv1.2_2021
- TLSv1.2_2019
- TLSv1.2_2018
- TLSv1.1_2016

Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies noch nicht geschehen ist:

- Erstellen Sie ein Lightsail-Netzwerk zur Inhaltsbereitstellung
- Erstellen von SSL-/TLS-Zertifikaten für Ihre Verteilung
- Validieren von SSL-/TLS-Zertifikaten für Ihre Verteilung
- Aktivieren benutzerdefinierter Domains für Ihre Verteilung
- Verweisen Sie mit Ihrer Domain auf den Vertrieb

Identifizieren Sie die Mindestversion des TLS-Protokolls für Ihre Distribution

Gehen Sie wie folgt vor, um die Mindestversion des TLS-Protokolls für Ihre Lightsail-Distribution zu ermitteln.

> **Note**
>
> In diesem Handbuch verwenden Sie, AWS CloudShell um das Upgrade durchzuführen. CloudShell ist eine browserbasierte, vorauthentifizierte Shell, die Sie direkt von der Lightsail-Konsole aus starten können. Mit CloudShell können Sie AWS CLI Befehle mit Ihrer bevorzugten Shell wie Bash oder Z-Shell ausführen. PowerShell Sie können dies tun, ohne Befehlszeilentools herunterladen oder installieren zu müssen. Weitere Informationen zur Einrichtung und Verwendung CloudShell finden Sie unter Weitere Informationen finden Sie unter AWS CloudShell Lightsail.

1. Öffnen Sie ein Terminal AWS CloudShell- oder Befehlszeilenfenster.

2. Geben Sie den folgenden Befehl ein, um die Mindestversion des TLS-Protokolls für Ihre Lightsail-Distribution zu ermitteln.

```
aws lightsail get-distributions --distribution-name DistributionName --region us-east-1 | grep "viewerMinimumTlsProtocolVersion"
```

Ersetzen Sie den Befehl *DistributionName*durch den Namen der Distribution, die Sie ändern möchten.

Beispiel

```
aws lightsail get-distributions --distribution-name Distribution-1 --region us-east-1 | grep "viewerMinimumTlsProtocolVersion"
```

Der Befehl gibt die ID der minimalen TLS-Protokollversion für Ihre Distribution zurück.

Beispiel

```
"viewerMinimumTlsProtocolVersion": "TLSv1.2_2021"
```

Konfigurieren Sie die minimale TLS-Protokollversion mit dem AWS CLI

Gehen Sie wie folgt vor, um die TLS-Protokollversion mithilfe von AWS Command Line Interface (AWS CLI) zu konfigurieren. Führen Sie dazu den Befehl `update-distribution` aus. Weitere Informationen finden Sie unter dem Attribut update-distribution in der AWS CLI Befehlsreferenz.

1. Öffnen Sie ein Terminal AWS CloudShell- oder Befehlszeilenfenster.
2. Geben Sie den folgenden Befehl ein, um die Mindestversion des TLS-Protokolls für Ihre Distribution zu ändern.

```
aws lightsail update-distribution --distribution-name DistributionName --viewer-minimum-tls-protocol-version ProtocolVersion
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *DistributionName*mit dem Namen der Distribution, die Sie aktualisieren möchten.
- *ProtocolVersion*mit der gültigen TLS-Protokollversion. Zum Beispiel `TLSv1.2_2021` oder `TLSv1.2_2019`.

Beispiel:

```
aws lightsail update-distribution --distribution-name  MyDistribution --viewer-
minimum-tls-protocol-version TLSv1.2_2021
```

Es dauert einen Moment, bis Ihre Änderung wirksam wird.

Löschen eines SSL-/TLS-Zertifikats für Ihre Lightsail-Verteilung

Sie können Amazon Lightsail SSL-/TLS-Zertifikate löschen, das Sie nicht mehr für Ihre Verteilungen verwenden. Beispielsweise könnte Ihr Zertifikat abgelaufen sein und Sie haben bereits ein aktualisiertes und validiertes Zertifikat zugewiesen. Weitere Informationen zu Zertifikaten finden Sie unter SSL-/TLS-Zertifikate in. Weitere Informationen zu Verteilungen finden Sie unter Netzwerkverteilungen für die Bereitstellung von Inhalten.

Löschen eines SSL-/TLS-Zertifikats ist endgültig und kann nicht rückgängig gemacht werden. Sie haben ein Kontingent für die Zertifikate, die Sie über einen Zeitraum von 365 Tagen erstellen können. Weitere Informationen finden Sie unter Lightsail Servicekontingente im Allgemeine AWS-Referenz.

Löschen eines SSL-/TLS-Zertifikats für die Verteilung

Vervollständigen Sie das folgende Verfahren, um ein SSL-/TLS-Zertifikat für die Verteilung zu löschen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen der Verteilung, aus der Sie das SSL-/TLS-Zertifikat löschen möchten. Wenn das Zertifikat derzeit nicht verwendet wird, können Sie eine beliebige Verteilung auswählen, da alle Ihre Zertifikate in jeder Verteilung aufgelistet sind.
4. Wählen Sie die Registerkarte Benutzerdefinierte Domänen auf der Verwaltungsseite Ihrer Verteilung aus.
5. Im Abschnitt Zertifikate auf der Seite, wählen Sie das Ellipsen-Symbol (⋮) für das Zertifikat, das Sie löschen möchten,und wählen Sie Löschen.

   DieLöschen-Option ist nicht verfügbar, wenn das Zertifikat, das Sie löschen möchten, in Verwendung ist. Um Zertifikate zu löschen, die in Verwendung sind, müssen Sie zuerst die

benutzerdefinierten Domänen der Verteilung ändern, die das Zertifikat verwenden, oder benutzerdefinierte Domänen in der Verteilung deaktivieren, die das Zertifikat verwenden. Weitere Informationen finden Sie unter Ändern benutzerdefinierter Domains für Ihre Verteilung und Aktivieren benutzerdefinierter Domains für Ihre Verteilungen.

6. Wählen Sie Yes, delete (Ja, löschen) zum Bestätigen der Löschung aus.

Objektspeicher in Amazon Lightsail

Verwenden Sie den Amazon Lightsail-Objektspeicherdienst, um jederzeit und von überall aus Objekte dem Internet zu speichern und abzurufen. Er wurde entwickelt, um Entwicklern die Datenverarbeitung im Web zu erleichtern, und basiert auf dem Amazon Simple Storage Service (Amazon S3). Lightsail-Objektspeicher ermöglicht Ihnen den Zugriff auf die gleiche hoch skalierbare, zuverlässige, schnelle und kostengünstige Datenspeicherinfrastruktur, die Amazon für den Betrieb seines eigenen globalen Netzwerks von Websites verwendet. Somit können auch Entwickler von den Vorteilen einer flexiblen Skalierbarkeit profitieren.

Konzepte für Objektspeicherklasse

Die folgenden Konzepte und Terminologie gelten für den Lightsail-Objektspeicher.

Buckets

Ein Bucket ist ein Container für Objekte, die im Lightsail-Objektspeicherdienst. Jedes Objekt ist in einem Bucket enthalten, der über eine eigene URL verfügt. Wenn beispielsweise ein Objekt mit dem Namen `media/sailbot.jpg` im Bucket `DOC-EXAMPLE-BUCKET` in der Region (`us-east-1`) USA Ost (Nord-Virginia) gespeichert ist, ist es über die URL adressierbar, die ähnlich mit `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg` ist.

Sie können Buckets in AWS-Regionen erstellen, in denen Lightsail verfügbar ist. Informationen über die AWS-Regionen, in denen Lightsail verfügbar ist, finden Sie unter Regionen und Endpunkte in der Allgemeinen AWS-Referenz.

Bucketspeichertarife

Ein Speichertarif, der in der AWS-API als Bündel bezeichnet wird, gibt die monatlichen Kosten, den Speicherplatz und das Datenübertragungskontingent für Ihren Bucket an. Sie müssen einen Speicherplan auswählen, wenn Sie den Bucket zum ersten Mal erstellen. Sie können es später ändern, nachdem Ihr Bucket betriebsbereit ist.

Sie können den Bucket-Plan innerhalb Ihres monatlichen AWS-Abrechnungszeitraums nur einmal ändern. Ändern Sie den Plan Ihres Buckets, wenn dieser konsistent über seinen Speicherplatz oder das Datenübertragungskontingent geht oder wenn die Nutzung Ihres Buckets konsistent im unteren Bereich des Speicherplatzes oder der Datenübertragungskontingents liegt. Da in Ihrem Bucket möglicherweise unvorhersehbare Nutzungsschwankungen auftreten, empfehlen wir Ihnen dringend,

den Plan Ihres Buckets nur als langfristige Strategie zu ändern, anstatt als kurzfristige, monatliche Kostensenkungsmaßnahme. Wählen Sie einen Speicherplan, der Ihrem Bucket ausreichend Speicherplatz und Datenübertragungsquoten für eine lange Zeit zur Verfügung stellt.

Objekte

Objekte sind die Grundeinheiten, die in Buckets gespeichert sind. Eine Datei, die Sie in Ihren Bucket hochladen, wird als Objekt bezeichnet, während sie gespeichert wird. Objekte bestehen aus Objekt- und Metadaten. Der Teil Daten ist für de nLightsail-Objektspeicherdienst nicht einsichtig. Metadaten bestehen aus mehreren Name/Wert-Paaren, die das Objekt beschreiben. Diese umfassen Standardmetadaten (z. B. das Datum der letzten Änderung), sowie Standard-HTTP-Metadaten (z. B. den Inhaltstyp).

Ein Objekt wird innerhalb eines Buckets eindeutig durch einen Schlüssel (Name) und eine Version-ID identifiziert.

Objektschlüsselnamen

Ein Schlüssel ist der eindeutige Bezeichner für ein Objekt in einem Bucket. Jedes Objekt in einem Bucket besitzt genau einen Schlüssel. Jedes Objekt wird durch die Kombination aus Bucket, Schlüssel und Version-ID eindeutig identifiziert. Lightsail-Objektspeicher fungiert also als grundlegende Datenzuordnung zwischen "Bucket + Schlüssel + Version" und dem Objekt selbst. Jedes Objekt im Lightsail-Objektspeicher ist über eine Kombination von Webservice-Endpunkt, Bucket-Name, Schlüssel und wahlweise einer Version aufrufbar. So ist in der URL `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg` `DOC-EXAMPLE-BUCKET` der Name des Buckets und `media/sailbot.jpg` der Name des Objektschlüssels.

Objekt-Versioning

Versioning ist eine Feature, mit der Sie mehrere Versionen eines Objekts im selben Bucket aufbewahren können. Aktivieren Sie Versioning, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Daten lassen sich dank Versioning nach unbeabsichtigten Benutzeraktionen und Anwendungsfehlern leichter wiederherstellen.

Standardmäßig ist die Versioning deaktiviert, wenn Sie einen Bucket erstellen. Nachdem Sie das Versioning aktiviert haben, wird jede Version jedes Objekts, das Sie in Ihrem Bucket speichern, beibehalten, bis Sie die gespeicherte Version manuell löschen. Wenn Sie beispielsweise das `media/sailbot.jpg`-Objekt und später eine größere Datei mit demselben Objektschlüsselnamen speichern, wird das ursprüngliche kleinere Objekt als Frühere Version beibehalten. Das neue,

größere Objekt wird die Aktuelle Version. Wenn Sie die vorherige Version des Objekts nicht benötigen, können Sie sie löschen. Alle gespeicherten früheren Versionen eines Objekts werden gelöscht, wenn Sie die aktuelle Version des Objekts löschen.

Gespeicherte Objektversionen belegen den Speicherplatz Ihres Buckets auf die gleiche Weise wie gespeicherte aktuelle Versionen eines Objekts. Nachdem Sie das Versioning aktiviert haben, können Sie sie anhalten, um die Speicherung von Objektversionen zu beenden. Dies verbraucht auch weniger Speicherplatz Ihres Buckets, wenn Sie neue Objektversionen hochladen. Wenn Sie das Versioning anhalten, werden gespeicherte Objektversionen beibehalten, neue Objektversionen, die Sie hochladen, während das Versioning angehalten wird, werden jedoch nicht beibehalten.

Zugriff auf Bucket und Objekt

Standardmäßig sind alle Objektspeicher-Ressourcen – Buckets und Objekte – privat. Das bedeutet, dass nur der Bucket-Eigentümer, das Lightsail-Konto, das es erstellt hat, auf den Bucket und seine Objekte zugreifen kann. Optional kann der Bucket-Eigentümer anderen Zugriffsberechtigungen gewähren. Dies kann getan werden, indem alle Objekte oder einzelne Objekte öffentlich eingestellt werden, wodurch sie für jeden auf der Welt lesbar sind. Sie können auch vollen programmatischen Zugriff gewähren, indem Sie Lightsail-Instance zu Ihrem Bucket hinzufügen oder indem Sie Zugriffsschlüssel für Ihren Bucket erstellen. Abschließend können Sie andere AWS-Konten programmgesteuerten schreibgeschützten Zugriff auf Ihren Bucket erteilen.

AWS-Regionen

Sie können Lightsail-Objektspeicher-Buckets in allen AWS-Regionen erstellen, in denen Lightsail vorhanden ist. Sie sollten eine Region im Hinblick auf Latenz, Kosten sowie Einhaltung der relevanten Vorschriften auswählen. In einer AWS-Region gespeicherte Objekte verbleiben in der Region, bis sie explizit in eine andere Region übertragen werden. So verlassen Objekte, die in der Region USA West (Oregon) gespeichert werden, diese Region nicht.

Verwalten von Buckets und Objekten

Der Lightsail-Objektspeicher wurde ursprünglich mit einer minimalen Feature menge angelegt, die einfach und robust sein sollte. Im Folgenden sind einige der Elemente der Verwaltung von Buckets und Objekten:

- Erstellen von Buckets – Buckets zum Speichern von Daten erstellen. Buckets sind die grundlegende Container im Lightsail-Objektspeicherdienst. Weitere Informationen finden Sie unter Einen Bucket erstellen.

- Daten speichern – Laden Sie Dateien mit der Lightsail-Konsole, der AWS Command Line Interface (AWS CLI) und AWS-APIs hoch. Weitere Informationen zum Hochladen von Dateien finden Sie auf Hochladen von Dateien auf einen Bucket.
- Daten herunterladen – Laden Sie Ihre gespeicherten Objekte jederzeit herunter. Weitere Informationen finden Sie unter Herunterladen von Objekten aus einem Bucket.
- Gewähren von Zugriff – Gewähren oder Verweigern des Zugriffs für andere (z. B. Software oder Einzelpersonen), die Daten aus Ihrem Bucket hochladen oder aus diesem herunterladen wollen. Authentifizierungsmechanismen können Ihnen helfen, Daten vor unbefugtem Zugriff zu schützen. Weitere Informationen finden Sie unter Bucketberechtigungen.
- Verwalten des Versioning – Aktivieren Sie Versioning, um alle Versionen aller Objekte in Ihrem Bucket zu speichern. Weitere Informationen finden Sie unter Aktivieren und Aussetzen der Bucket-Objekt-Versionsverwaltung.
- Überwachen der Nutzung – Überwachen Sie die Anzahl der in Ihrem Bucket gespeicherten Objekte und den belegten Speicherplatz. Weitere Informationen finden Sie unter Anzeigen von Bucket-Metriken.
- Ändern des Speicherplans – Vergrößern Sie Ihren Bucket, wenn er übermäßig ausgelastet wird, oder verkleinern Sie ihn, wenn er nicht ausgelastet wird. Weitere Informationen finden Sie unter Ändern des Tarifs Ihres Buckets.
- Verbinden Ihres Buckets – Verbinden Sie Ihr Lightsail-Bucket mit Ihrer WordPress Website, um Website-Images und Anhänge zu speichern. Sie können Ihren Bucket auch als Ursprung einer Lightsail-Verteilung für Bereitstellung von Inhalten (CDN). Dies beschleunigt die Lieferung von Objekten in Ihrem Bucket an Ihre Benutzer auf der ganzen Welt. Weitere Informationen finden Sie unter Tutorial: Verbinden Ihrer WordPress-Instance mit einem Bucket und Tutorial: Verwenden eines Buckets mit einer Netzwerkverteilung für die Bereitstellung von Inhalten.
- Löschen des Buckets – Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen eines Buckets.

Erstellen eines Lightsail-Buckets

Erstellen Sie einen Bucket im Amazon Lightsail-Objektspeicherdienst, wenn Sie bereit sind anzufangen, Ihre Dateien in die Cloud hochzuladen. Jede Datei, die Sie in den Lightsail-Objektspeicherdienst hochladen, wird in einemLightsail-Bucket gespeichert. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Erstellen eines -Buckets

Führen Sie das folgende Verfahren durch, um einen Lightsail-Bucket zu erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie Create Bucket (Bucket erstellen) aus.
4. Wählen Sie AWS-Region ändern aus, um die Region, in der Sie Ihren Bucket erstellen möchten auszuwählen.

   Wir raten Ihnen, Ihren Bucket in derselben AWS-Region zu erstellen, in der sich die Ressourcen befinden, die Sie mit Ihrem Bucket verwenden möchten. Sobald Ihr Bucket erstellt ist, kann die Region nicht nachträglich geändert werden.
5. Wählen Sie einen Speicherplan für Ihren Bucket aus.

   Der Speicherplan gibt die monatlichen Kosten, das Speicherplatzkontingent und das Datenübertragungskontingent für Ihren Bucket an.

   Sie können den Bucket-Plan innerhalb Ihres monatlichen AWS-Abrechnungszeitraums nur einmal ändern. Ändern Sie den Plan Ihres Buckets, wenn dieser konsistent über seinen Speicherplatz oder das Datenübertragungskontingent geht oder wenn die Nutzung Ihres Buckets konsistent im unteren Bereich des Speicherplatzes oder der Datenübertragungskontingents liegt. Weitere Informationen finden Sie unter Ändern des Plans Ihres Buckets.
6. Geben Sie einen Namen für Ihren Bucket ein.

   Weitere Informationen zu Bucket-Namen finden Sie unter Regeln für die Bucket-Benennung inAmazon Lightsail.
7. Wählen Sie Create Bucket (Bucket erstellen) aus.

   Sie werden zur Verwaltungsseite Ihres neuen Buckets umgeleitet. Für weitere Unterlagen zum Verwenden und Verwalten Ihres Buckets, fahren Sie mit dem Abschnitt „Nächste Schritte“ in diesem Leitfaden fort.

Verwalten von Buckets und Objekten

Dies sind die allgemeinen Schritte zum Verwalten Ihres Lightsail-Objektspeicher-Buckets:

1. Weitere Informationen über Buckets und Objekte im Amazon Lightsail-Objektspeicherservice. Weitere Informationen zu Buckets finden Sie unter Objektspeicher in Amazon Lightsail.
2. Erfahren Sie mehr über die Namen, die Sie Ihren Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Namensregeln für Buckets in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherservice, indem Sie einen Bucket erstellen. Weitere Informationen finden Sie unter Buckets erstellen in Amazon Lightsail.
4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Lightsail-Objektspeicher und Bucket-Berechtigungen in Amazon Lightsail verstehen.

   Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

   - Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail
   - Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail
   - Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
   - Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
   - Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail
   - Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail
5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.

   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherservice
   - Zugriffsprotokollierungsformat für Buckets im Amazon Lightsail-Objektspeicher-Service
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicher-Service
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail, um Anforderungen zu identifizieren

6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gewährt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets in Amazon Lightsail.
7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unterGrundlegendes zu Objektschlüsselnamen inAmazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Hochladen einer Datei in einen Bucket in Amazon Lightsail
   - Hochladen von Dateien in Buckets in Amazon Lightsail mit mehrteiligem Upload
   - Anzeigen von Objekten in einem Bucket in Amazon Lightsail
   - Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
   - Objekte von einem Bucket in Amazon Lightsail herunterladen
   - Filtern von Objekten in einem Bucket in Amazon Lightsail
   - Markieren von Objekten in einem Bucket in Amazon Lightsail
   - Löschen von Objekten in einem Bucket in Amazon Lightsail
9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.
10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.
11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.
12. Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen in Amazon Lightsail.
13. Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Tarifs Ihres Buckets in Amazon Lightsail.
14. Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.
   - Tutorial: Verbinden einer WordPress-Instance mit einem Amazon Lightsail-Bucket

- Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Lightsail-Netzwerkverteilung für die Bereitstellung von Inhalten

15 Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

Löschen eines Lightsail-Buckets

Löschen Sie Ihren Bucket imAmazon LightsailObjectspeicherdienst, wenn Sie ihn nicht mehr verwenden. Wenn Sie den Bucket löschen, werden alle Objekte im Bucket, einschließlich gespeicherter Versionen von Objekten und Zugriffsschlüsseln, endgültig gelöscht.

Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Zwangslöschen eines Buckets

Buckets mit einer der folgenden Bedingungen können nur gelöscht werden, wenn Sie den Löschvorgang bestätigen:

- Der Bucket ist der Ursprung einer Verteilung.
- Dem Bucket sind Instances angefügt.
- Der Bucket verfügt über Objekte.
- Der Bucket hat Zugriffsschlüssel.

Sie müssen den Löschvorgang bestätigen, um sicherzustellen, dass Sie einen vorhandenen Workflow, der auf dem Bucket basiert, nicht unterbrechen. Zum Beispiel eine WordPress-Website, die Medien im Bucket speichert, oder eine Verteilung, die Objekte in Ihrem Bucket zwischenspeichert und bereitstellt.

Um das Löschen eines Buckets zu bestätigen, der eine der vorhergehenden Bedingungen aufweist, müssen Sie das Löschen des Buckets erzwingen. Bevor Sie den Bucket löschen, wird derLightsail-Dienst Sie fragen, welche dieser Bedingungen für den Bucket vorhanden sind. Wenn Sie dieLightsail-Konsole verwenden, um Ihren Bucket zu löschen, wird Ihnen die Option angezeigt, das Löschen zu erzwingen. Wenn Sie die AWS CLI verwenden, müssen Sie das `--force-delete`-Flag beim Erstellen einer `delete-bucket`-Anforderung angeben. Beide Verfahren werden in den Abschnitten Löschen Sie Ihren Bucket mit derLightsail-KonsoleundLöschen Sie Ihren Bucket mit denAWS CLI dieses Leitfadens behandelt.

Löschen Ihres Buckets mit der Lightsail-Konsole

Vervollständigen Sie den folgenden Vorgang, um den Bucket mit derLightsail-Konsole zu löschen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen des Buckets aus, den Sie löschen möchten.
4. Wählen Sie das Ellipsen-Symbol (⋮) im Registerkarten-Menü und wählen Sie dann Löschen aus.
5. Wählen Sie Bucket löschen aus.
6. Bestätigen Sie in der angezeigten Eingabeaufforderung, falls Ihr Bucket eine der folgenden Bedingungen erfüllt:

   - Enthält ein Objekt
   - Enthält Zugriffsschlüssel
   - Ist einer Instance angefügt
   - Ist der Ursprung einer Verteilung

   Wenn eine dieser Bedingungen erfüllt ist, müssen Sie das Löschen des Buckets erzwingen.
7. Wählen Sie eine der folgenden Optionen:

   - Wählen Sie Löschen erzwingen, um Ihren Bucket zu löschen, auch wenn er eine der Bedingungen erfüllt, die in Schritt 6 dieses Verfahrens aufgeführt sind.
   - Wählen Sie Löschen erzwingen, um Ihren Bucket zu löschen, wenn er keine der Bedingungen erfüllt, die in Schritt 6 dieses Verfahrens aufgeführt sind.
   - Wählen SieNein, abbrechenum das Löschen abzubrechen.

Löschen Ihres Buckets mit der AWS CLI

Vervollständigen Sie den folgenden Vorgang, um den Bucket mit der AWS Command Line Interface (AWS CLI) zu löschen. Führen Sie dazu den Befehl `delete-bucket` aus. Weitere Informationen finden Sie unter delete-bucket in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie in der Eingabeaufforderung oder im Terminalfenster einen der folgenden Befehle ein:

   - Geben Sie den folgenden Befehl ein, um einen Bucket zu löschen, der nicht die Bedingungen erfüllt, die im Abschnitt Löschen eines Buckets erzwingen in diesem Leitfaden aufgeführt sind.

     ```
     aws lightsail delete-bucket --bucket-name BucketName
     ```

   - Geben Sie den folgenden Befehl ein, um einen Bucket zu löschen, der die Bedingungen erfüllt, die im Abschnitt Löschen eines Buckets erzwingen in diesem Leitfaden aufgeführt sind.

     ```
     aws lightsail delete-bucket --bucket-name BucketName --force-delete
     ```

   Ersetzen Sie in den Befehlen,*Bucket-Name*mit dem Namen des Buckets, den Sie löschen möchten.

   Beispiel:

   ```
   aws lightsail delete-bucket --bucket-name DOC-EXAMPLE-BUCKET
   ```

   Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

```
C:\>aws lightsail delete-bucket --bucket-name DOC-EXAMPLE-BUCKET
{
    "operations": [
        {
            "id": "6example-4d30-4442-ae9a-examplef4f52",
            "resourceName": "DOC-EXAMPLE-BUCKET",
            "resourceType": "Bucket",
            "createdAt": "2021-06-30T13:42:43.873000-07:00",
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "62example362/DOC-EXAMPLE-BUCKET/small_1_0",
            "operationType": "DeleteBucket",
            "status": "Succeeded",
            "statusChangedAt": "2021-06-30T13:42:43.873000-07:00",
            "errorCode": "",
            "errorDetails": ""
        }
    ]
}
```

Verwalten von Buckets und Objekten

Dies sind die allgemeinen Schritte zum Verwalten Ihres Lightsail-Objektspeicher-Buckets:

1. Weitere Informationen über Buckets und Objekte im Amazon Lightsail-Objektspeicherservice. Weitere Informationen zu Buckets finden Sie unter Objektspeicher in Amazon Lightsail.
2. Erfahren Sie mehr über die Namen, die Sie Ihren Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Namensregeln für Buckets in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherservice, indem Sie einen Bucket erstellen. Weitere Informationen finden Sie unter Buckets erstellen in Amazon Lightsail.
4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Lightsail-Objektspeicher und Bucket-Berechtigungen in Amazon Lightsail verstehen.

Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

- Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail
- Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail
- Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
- Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
- Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail
- Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail

5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherservice
   - Zugriffsprotokollierungsformat für Buckets im Amazon Lightsail-Objektspeicher-Service
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicher-Service
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail, um Anforderungen zu identifizieren
6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gewährt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets in Amazon Lightsail.
7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unterGrundlegendes zu Objektschlüsselnamen inAmazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Hochladen einer Datei in einen Bucket in Amazon Lightsail
   - Hochladen von Dateien in Buckets in Amazon Lightsail mit mehrteiligem Upload
   - Anzeigen von Objekten in einem Bucket in Amazon Lightsail
   - Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
   - Objekte von einem Bucket in Amazon Lightsail herunterladen
   - Filtern von Objekten in einem Bucket in Amazon Lightsail
   - Markieren von Objekten in einem Bucket in Amazon Lightsail

- Löschen von Objekten in einem Bucket in Amazon Lightsail

9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.
10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.
11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.
12. Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen in Amazon Lightsail.
13. Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Tarifs Ihres Buckets in Amazon Lightsail.
14. Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.
    - Tutorial: Verbinden einer WordPress-Instance mit einem Amazon Lightsail-Bucket
    - Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Lightsail-Netzwerkverteilung für die Bereitstellung von Inhalten
15. Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

Erstellen von Lightsail-Bucket-Zugriffsschlüsseln

Verwenden Sie Zugriffsschlüssel, um eine Gruppe von Anmeldeinformationen zu erstellen, die vollen Zugriff auf einen Bucket und seine Objekte gewähren. Sie können Zugriffsschlüssel für Ihre Software oder Ihr Plugin so konfigurieren, dass sie vollen Lese- und Schreibzugriff auf einen Bucket mit dem AWS-APIs und AWS-SDKs haben. Sie können Zugriffsschlüssel auch mit der AWS CLI konfigurieren.

Access keys (Zugriffsschlüssel) bestehen sowie aus einer Access keys (Zugriffsschlüssel)-ID als auch aus einem geheimen Access keys (Zugriffsschlüssel). Der geheime Zugriffsschlüssel ist nur sichtbar, wenn Sie ihn erstellen. Wenn Ihr geheimer Zugriffsschlüssel kopiert wurde, verloren geht oder kompromittiert wird, sollten Sie Ihren Zugriffsschlüssel löschen und einen neuen erstellen.

Sie können maximal zwei Zugriffsschlüssel pro Bucket besitzen. Obwohl Sie zwei haben können, ist es nützlich, einen Zugriffsschlüssel für Ihren Bucket zu haben, wenn Sie den Schlüssel drehen müssen. Um einen Zugriffsschlüssel zu drehen, erstellen Sie einen neuen, konfigurieren Sie ihn in Ihrer Software und testen Sie ihn. Löschen Sie dann den vorherigen Schlüssel. Das Löschen eines Zugriffsschlüssels ist ein endgültiger Vorgang, der nicht rückgängig gemacht werden kann. Er kann nur durch einen neuen Zugriffsschlüssel ersetzt werden.

Weitere Informationen zu Berechtigungsoptionen finden Sie unter Bucket-Berechtigungen. Weitere Informationen zu bewährten Methoden für die Sicherheit finden Sie unter Bewährte Methoden für die Sicherheit für Objektspeicher. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Erstellen von Zugriffsschlüsseln für einen Bucket

Führen Sie das folgende Verfahren durch, um Zugriffsschlüssel für einen Bucket zu erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen des Buckets aus, für den Sie Zugriffsberechtigungen konfigurieren möchten.
4. Wählen Sie die Registerkarte Permissions (Berechtigungen).

   Im Abschnitt Access keys (Zugriffsschlüssel) der Seite werden die vorhandenen Zugriffsschlüssel für den Bucket angezeigt, falls vorhanden.
5. Wählen Sie Create access key (Zugriffsschlüssel erstellen) aus, um einen neuen Schlüssel für den Bucket zu erstellen.

   > **Note**
   >
   > Sie können auch auswählen, einen vorhandenen Zugriffsschlüssel zu löschen, indem Sie das Papierkorb-Symbol für den Schlüssel auswählen, den Sie löschen möchten.
6. Wählen Sie in der angezeigten EingabeaufforderungYes, Create (Ja, erstellen) aus, um zu bestätigen, dass Sie einen neuen Zugriffsschlüssel erstellen möchten. Andernfalls wählen Sie Nein, abbrechen.
7. Notieren Sie sich in der angezeigten Eingabeaufforderung die Zugriffsschlüssel-ID.
8. Wählen Sie Geheimer Zugriffsschlüssel anzeigen, um den geheimen Zugriffsschlüssel anzuzeigen, und notieren Sie ihn. Der geheime Zugriffsschlüssel wird nicht wieder angezeigt.

> **Important**
>
> Speichern Sie Ihre Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel an einem sicheren Ort. Wenn es kompromittiert wird, sollten Sie ihn löschen und einen neuen erstellen.

9. Wählen SieWeiter um den Vorgang abzuschließen.

   Der neue Access keys (Zugriffsschlüssel) wird im Abschnitt Access keys (Zugriffsschlüssel) der Seite aufgelistet. Wenn Ihr Zugriffsschlüssel komprimittiert wird oder verloren geht, löschen Sie ihn und erstellen Sie einen neuen.

> **Note**
>
> Die Spalte Zuletzt verwendet, die neben jedem Zugriffsschlüssel angezeigt wird, gibt an, wann der Schlüssel zuletzt verwendet wurde. Ein Bindestrich wird angezeigt, wenn der Schlüssel nicht verwendet wurde. Erweitern Sie den Zugriffsschlüssel-Knoten, um den Service und die AWS-Region anzuzeigen, in der der Schlüssel zuletzt verwendet wurde.

Blockieren des öffentlichen Zugriffs auf Lightsail-Buckets

Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, bei dem Kunden Daten speichern und schützen können. Der Amazon Lightsail-Objektspeicherservice basiert auf der Amazon-S3-Technologie. Amazon S3 bietet das Blockieren des öffentlichen Zugriffs auf Kontoebene, um den öffentlichen Zugriff auf alle S3-Buckets in einem AWS-Konto zu beschränken. Das Blockieren des öffentlichen Zugriffs auf Kontoebene kann alle S3-Buckets in einem AWS-Konto auf privat einstellen, unabhängig von den bestehenden einzelnen Bucket- und Objektberechtigungen.

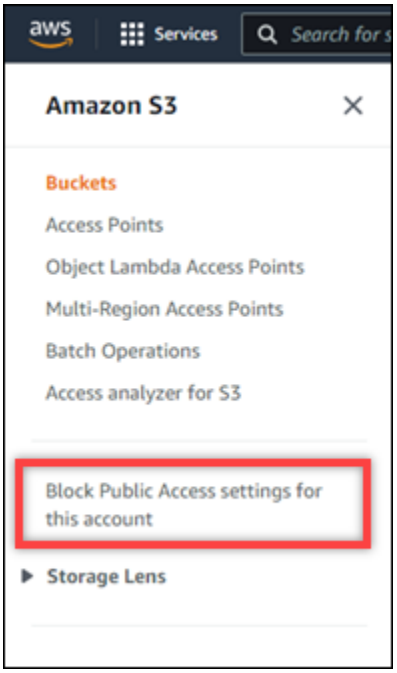
Beim Zulassen oder Verweigern des öffentlichen Zugriffs berücksichtigen Lightsail-Objektspeicher-Buckets Folgendes:

- Zugriffsberechtigungen für Lightsail-Buckets. Weitere Informationen finden Sie unter Bucketberechtigungen.
- Konfigurationen für die Sperrung des öffentlichen Zugriffs auf Amazon-S3-Kontoebene, die die Zugriffsberechtigungen für den Lightsail-Bucket außer Kraft setzen.

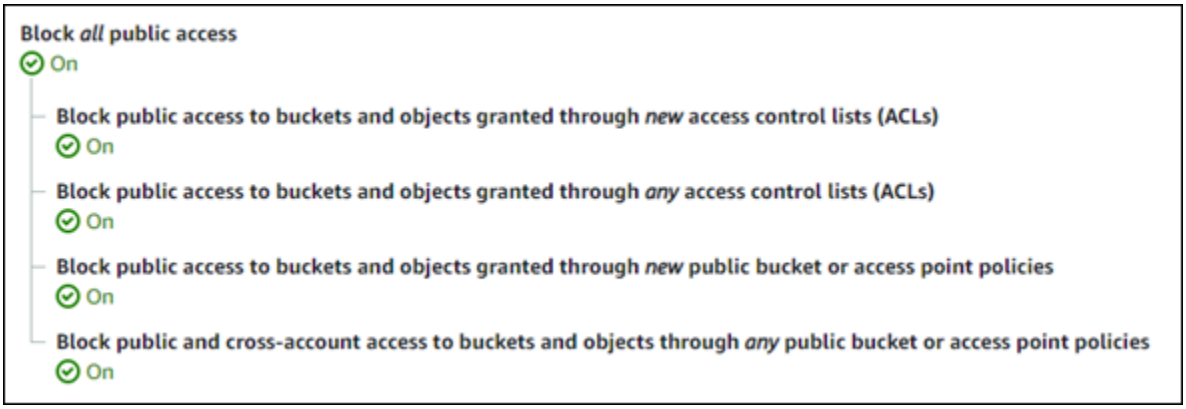
Das heißt, wenn Sie Den gesamten öffentlichen Zugriff blockieren in Amazon S3 aktivieren, werden Ihre öffentlichen Lightsail-Buckets und -Objekte privat und sind nicht mehr öffentlich zugänglich.

Konfigurieren der Block-Public-Access-Einstellungen für Ihr Konto

Sie können die Amazon-S3-Konsole, AWS Command Line Interface (AWS CLI), AWS-SDKs und die REST-API verwenden, um Einstellungen für das Blockieren des öffentlichen Zugriffs zu konfigurieren. Sie können auf das Feature zum Sperren des öffentlichen Zugriffs auf Kontoebene im Navigationsbereich der Amazon-S3-Konsole zugreifen, wie im folgenden Beispiel gezeigt.



Die Amazon-S3-Konsole bietet Einstellungen zum Blockieren des gesamten öffentlichen Zugriffs, zum Blockieren des öffentlichen Zugriffs, der über neue oder beliebige Zugriffskontrolllisten gewährt wird, und zum Blockieren des öffentlichen Zugriffs auf Buckets und Objekte, der durch neue oder öffentliche Bucket- oder Zugriffspunktrichtlinien gewährt wird.



Sie können jede Einstellung in der Amazon-S3-Konsole auf Ein oder Aus stellen. In der API ist die entsprechende Einstellung `TRUE` (Ein) oder `FALSE` (Aus). In den folgenden Abschnitten werden die Auswirkungen der einzelnen Einstellungen auf S3-Buckets und Lightsail-Buckets beschrieben.

> **Note**
>
> In den folgenden Abschnitten werden Zugriffskontrolllisten (Access Control Lists, ACLs) erwähnt. Eine ACL definiert die Benutzer, die einen Bucket oder einzelne Objekte besitzen oder darauf zugreifen können. Weitere Informationen finden Sie unter Zugriffssteuerungslisten – Übersicht im Amazon-S3-Benutzerhandbuch.

- Den gesamten öffentlichen Zugriff blockieren – Aktivieren Sie diese Einstellung, um den gesamten öffentlichen Zugriff auf Ihre S3-Buckets, Lightsail-Buckets und die entsprechenden Objekte zu blockieren. Diese Einstellung beinhaltet alle folgenden Einstellungen. Wenn Sie diese Einstellung aktivieren, dürfen nur Sie (der Bucket-Besitzer) und autorisierte Benutzer auf Ihre Buckets und deren Objekte zugreifen. Sie können diese Einstellung nur in der Amazon-S3-Konsole aktivieren. Sie ist in der AWS CLI, der Amazon-S3-API oder AWS-SDKs nicht verfügbar.
  - Den öffentlichen Zugriff auf Buckets und Objekte, der durch neue Zugriffssteuerungslisten (ACL) gewährt wird, blockieren – Aktivieren Sie diese Einstellung, um zu verhindern, dass öffentliche ACLs auf Buckets und Objekten platziert werden. Diese Einstellung wirkt sich nicht auf bestehende ACLs aus. Daher bleibt ein Objekt, das bereits über eine öffentliche ACL verfügt, öffentlich. Diese Einstellung hat auch keine Auswirkung auf Objekte, die dadurch öffentlich sind, dass eine Bucket-Zugriffsberechtigung auf All objects are public and read-only (Alle Objekte sind öffentlich und schreibgeschützt) eingestellt ist. Diese Einstellung ist in der Amazon-S3-API als `BlockPublicAcls` gekennzeichnet.

    > **Note**
    >
    > WordPress-Plugins, die Medien in Lightsail-Buckets platzieren, wie das Offload-Media-Light-Plugin, funktionieren möglicherweise nicht mehr, wenn diese Einstellung aktiviert ist. Das liegt daran, dass die meisten WordPress-Plugins die öffentlich lesbare ACL für Objekte konfigurieren. WordPress-Plugins, die Objekt-ACLs umschalten, funktionieren möglicherweise ebenfalls nicht mehr.

  - Den öffentlichen Zugriff auf Buckets und Objekte, der durch beliebige Zugriffssteuerungslisten (ACL) gewährt wird, blockieren – Aktivieren Sie diese Einstellung, um öffentliche ACLs zu

ignorieren und den öffentlichen Zugriff auf Buckets und Objekte zu blockieren. Mit dieser Einstellung können öffentliche ACLs auf Buckets und Objekten platziert werden, sie werden jedoch ignoriert, wenn Zugriff gewährt wird. Für Lightsail-Buckets entspricht das Einstellen der Zugriffsberechtigung eines Bucket auf All objects are public and read-only (Alle Objekte sind öffentlich und schreibgeschützt) oder das Einstellen der Berechtigung eines einzelnen Objekts auf Public (read-only) (Öffentlich (schreibgeschützt)) dem Platzieren einer öffentlichen ACL auf dem Bucket bzw. dem Objekt. Diese Einstellung ist in der Amazon-S3-API als `IgnorePublicAcls` gekennzeichnet.

- Den öffentlichen Zugriff auf Buckets und Objekte, der durch neue Richtlinien für öffentliche Buckets oder Zugriffspunkte gewährt wird, blockieren – Aktivieren Sie diese Einstellung, um zu verhindern, dass die Bucket-Zugriffsberechtigung Alle Objekte sind öffentlich und schreibgeschützt auf Ihren Lightsail-Buckets konfiguriert wird. Diese Einstellung wirkt sich nicht auf Buckets aus, die bereits mit der Bucket-Zugriffsberechtigung All objects are public and read-only (Alle Objekte sind öffentlich und schreibgeschützt) konfiguriert sind. Diese Einstellung ist in der Amazon-S3-API als `BlockPublicPolicy` gekennzeichnet.
- Den öffentlichen und kontoübergreifenden Zugriff auf Buckets und Objekte durch jegliche Richtlinien für öffentliche Buckets oder Zugriffspunkte blockieren – Aktivieren Sie diese Einstellung, um alle Lightsail-Buckets auf privat einzustellen. Dadurch werden alle Lightsail-Buckets privat, auch wenn sie mit der Bucket-Zugriffsberechtigung All objects are public and read-only (Alle Objekte sind öffentlich und schreibgeschützt) konfiguriert sind. Diese Einstellung ist in der Amazon-S3-API als `RestrictPublicBuckets` gekennzeichnet.

  > **Important**
  >
  > Diese Einstellung blockiert auch den kontoübergreifenden Zugriff, der auf einem Lightsail-Bucket konfiguriert ist, der auch mit dem Bucket-Zugriffsberechtigung All objects are public and read-only (Alle Objekte sind öffentlich und schreibgeschützt) in Lightsail konfiguriert ist. Um den kontoübergreifenden Zugriff weiterhin zuzulassen, müssen Sie den Lightsail-Bucket mit der Bucket-Zugriffsberechtigung Alle Objekte sind privat in Lightsail konfigurieren, bevor Sie die Einstellung Den öffentlichen und kontoübergreifenden Zugriff auf Buckets und Objekte durch jegliche Richtlinien für öffentliche Buckets oder Zugriffspunkte blockieren in Amazon S3 aktivieren.

Weitere Informationen zum Blockieren des öffentlichen Zugriffs und zur Konfiguration finden Sie in den folgenden Ressourcen im Amazon-S3-Benutzerhandbuch:

- Blockieren des öffentlichen Zugriffs auf Ihren Amazon S3-Speicher
- Konfigurieren der Block-Public-Access-Einstellungen für Ihr Konto

Verwenden Sie die Lightsail-Konsole, AWS CLI, AWS SDKs und die REST-API zum Konfigurieren der Zugriffsberechtigungen für Ihre Lightsail-Buckets. Weitere Informationen finden Sie unter Bucketberechtigungen.

> **Note**
>
> Lightsail verwendet eine serviceverknüpfte Rolle, um die aktuelle Konfiguration für das Blockieren des öffentlichen Zugriffs auf Kontoebene von Amazon S3 zu erhalten und es auf Lightsail-Objektspeicher-Ressourcen anzuwenden. Warten Sie nach der Konfiguration der Blockierung des öffentlichen Zugriffs in Amazon S3 mindestens eine Stunde, bis sie in Lightsail wirksam wird. Weitere Informationen finden Sie unter Serviceverknüpfte Rollen.

Verwalten von Buckets und Objekten

Dies sind die allgemeinen Schritte zum Verwalten Ihres Lightsail-Objektspeicher-Buckets:

1. Weitere Informationen über Buckets und Objekte im Amazon Lightsail-Objektspeicherservice. Weitere Informationen zu Buckets finden Sie unter Objektspeicher in Amazon Lightsail.
2. Erfahren Sie mehr über die Namen, die Sie Ihren Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Namensregeln für Buckets in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherservice, indem Sie einen Bucket erstellen. Weitere Informationen finden Sie unter Buckets erstellen in Amazon Lightsail.
4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Lightsail-Objektspeicher und Bucket-Berechtigungen in Amazon Lightsail verstehen.

   Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

- Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail
- Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail
- Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
- Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
- Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail
- Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail

5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherservice
   - Zugriffsprotokollierungsformat für Buckets im Amazon Lightsail-Objektspeicher-Service
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicher-Service
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail, um Anforderungen zu identifizieren
6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gewährt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets in Amazon Lightsail.
7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unterGrundlegendes zu Objektschlüsselnamen inAmazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Hochladen einer Datei in einen Bucket in Amazon Lightsail
   - Hochladen von Dateien in Buckets in Amazon Lightsail mit mehrteiligem Upload
   - Anzeigen von Objekten in einem Bucket in Amazon Lightsail
   - Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
   - Objekte von einem Bucket in Amazon Lightsail herunterladen
   - Filtern von Objekten in einem Bucket in Amazon Lightsail
   - Markieren von Objekten in einem Bucket in Amazon Lightsail
   - Löschen von Objekten in einem Bucket in Amazon Lightsail

9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.
10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.
11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.
12. Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen in Amazon Lightsail.
13. Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Tarifs Ihres Buckets in Amazon Lightsail.
14. Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.
    - Tutorial: Verbinden einer WordPress-Instance mit einem Amazon Lightsail-Bucket
    - Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Lightsail-Netzwerkverteilung für die Bereitstellung von Inhalten
15. Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

Bucket-Zugriffsprotokolle in Amazon Lightsail

Die Zugriffsprotokollierung stellt detaillierte Aufzeichnungen für die Anforderungen bereit, die an einen Bucket im Amazon Lightsail-Objektspeicher-Service gestellt werden. Dabei kann es sich um den Anforderungstyp, die in der Anfrage angegebenen Ressourcen sowie Uhrzeit und Datum der Anfrageverarbeitung handeln. Zugriffsprotokolle sind für viele Anwendungen nützlich. Beispielsweise können Zugriffsprotokoll-Informationen bei Sicherheits- und Zugriffsprüfungen nützlich sein. Es kann Ihnen auch dabei helfen, mehr über Ihren Kundenstamm zu erfahren.

Inhalt

- Wie werden Protokolle ausgeliefert?
- Best-Effort-Protokollbereitstellung
- Statusänderungen in der Bucket-Protokollierung werden mit der Zeit wirksam

Was benötige ich, um die Protokollbereitstellung zu aktivieren?

Berücksichtigen Sie Folgendes, bevor Sie die Protokollbereitstellung aktivieren. Mehr Informationen finden Sie unter Zugriffsprotokollierung für einen Bucket aktivieren.

1. Identifizieren Sie den Ziel-Bucket für die Protokolle. In diesem Bucket soll Lightsail die Zugriffsprotokolle als Objekte speichern. Sowohl der Quell- als auch der Ziel-Bucket müssen sich in derselben AWS-Region befinden und demselben Konto gehören.

   Sie können Protokolle in jeden Bucket speichern lassen, der sich in der gleichen Region wie der Quell-Bucket befindet, einschließlich des Quell-Buckets selbst. Zur einfacheren Protokollverwaltung empfehlen wir jedoch, Zugriffsprotokolle in einem anderen Bucket zu speichern.

   Wenn der Quell- und Ziel-Bucket derselbe sind, werden zusätzliche Protokolle für die Protokolle erstellt, die in den Bucket geschrieben werden. Dies ist möglicherweise nicht ideal, da dies zu einer geringfügigen Erhöhung des Speicherverbrauchs führen könnte. Weiterhin könnten die zusätzlichen Protokolle über Protokolle das Auffinden des gesuchten Protokolls erschweren. Wenn Sie Zugriffsprotokolle im Quell-Bucket speichern, empfehlen wir Ihnen, ein Präfix für die Protokollobjektschlüssel anzugeben, damit die Objektnamen mit einer gemeinsamen Zeichenfolge beginnen und die Protokollobjekte leichter zu identifizieren sind. Schlüsselpräfixe sind auch nützlich, um zwischen Quell-Buckets zu unterscheiden, wenn mehrere Buckets im selben Ziel-Bucket protokolliert werden.
2. (Optional) Identifizieren Sie ein Präfix für die Protokollobjektschlüssel. Das Präfix macht es Ihnen einfacher, die Protokollobjekte zu finden. Wenn Sie beispielsweise den Präfixwert `logs/` angeben, beginnt jedes von Lightsail erstellte Protokollobjekt mit dem Präfix `logs/` in seinem Schlüssel. Der nachfolgende Schrägstrich `/` ist erforderlich, um das Ende des Präfixes zu kennzeichnen. Es folgt ein Beispiel für einen Protokollobjektschlüssel mit dem `logs/`-Präfix:

   ```
   logs/2021-11-31-21-32-16-E568B2907131C0C0
   ```

Protokollobjekt-Schlüsselformat

Lightsail verwendet das folgende Objektschlüsselformat für die Protokollobjekte, die in den Ziel-Bucket hochgeladen werden:

```
TargetPrefix/YYYY-mm-DD-HH-MM-SS-UniqueString
```

Im Schlüssel sind YYYY, `mm`, `DD`, `HH`, `MM` und `SS` die Ziffern von Jahr, Monat, Tag, Stunde, Minute bzw. Sekunden des Zeitpunkts, an dem die Protokolldatei übermittelt wurde. Datum und Uhrzeit entsprechen der Zeitzone UTC (Coordinated Universal Time).

Eine Protokolldatei, die zu einem bestimmten Zeitpunkt bereitgestellt wurde, kann Datensätze enthalten, die an einem beliebigen Zeitpunkt davor geschrieben wurden. Es lässt sich nicht feststellen, ob alle Protokoll-Datensätze für ein bestimmtes Zeitintervall bereitgestellt wurden oder nicht.

Die `UniqueString`-Komponente des Schlüssels verhindert, dass Dateien überschrieben werden. Sie hat keine Bedeutung und wird normalerweise von Protokollverarbeitungssoftware ignoriert.

Wie werden Protokolle ausgeliefert?

Lightsail sammelt periodisch Zugriffsprotokoll-Datensätze, fasst die Datensätze in Protokolldateien zusammen und lädt anschließend die Protokolldateien als Protokollobjekte in Ihren Ziel-Bucket hoch. Wenn Sie die Protokollierung bei mehreren Quell-Buckets aktivieren, die denselben Ziel-Bucket haben, werden die Zugriffsprotokolle für alle diese Quell-Buckets in diesen Ziel-Bucket geladen. Jedes Protokollobjekt gibt jedoch Zugriffsprotokoll-Datensätze für einen bestimmten Quell-Bucket aus.

Best-Effort-Protokollbereitstellung

Zugriffsprotokoll-Datensätze werden auf Best-Effort-Basis bereitgestellt. Die meisten Anforderungen nach einem Bucket, der für die Protokollierung richtig konfiguriert ist, führen zu einem ausgelieferten Protokollsatz. Die meisten Protokollsätze werden innerhalb weniger Stunden nach der Aufnahme geliefert, können aber häufiger geliefert werden.

Die Vollständigkeit und Aktualität der Zugriffsprotokollierung wird nicht garantiert. Der Protokolldatensatz für eine bestimmte Anforderung wird möglicherweise viel später bereitgestellt, als die Anforderung tatsächlich verarbeitet wurde; es kann auch sein, dass er gar nicht bereitgestellt wird. Der Zweck der Zugriffsprotokolle besteht darin, Ihnen einen Überblick über die Art des Datenverkehrs

zu und von Ihrem Bucket zu vermitteln. Es passiert selten, das Protokolldatensätze verloren gehen, aber die Zugriffsprotokollierung ist nicht als vollständige Auflistung aller Anfragen vorgesehen.

Statusänderungen in der Bucket-Protokollierung werden mit der Zeit wirksam

Änderungen am Protokollierungsstatus eines Buckets benötigen einige Zeit, bis sie sich auf die Bereitstellung von Protokolldateien auswirken. Wenn Sie beispielsweise die Protokollierung für einen Bucket aktivieren, werden möglicherweise einige Anforderungen, die in der darauffolgenden Stunde gemacht werden, protokolliert, andere hingegen nicht. Wenn Sie den Ziel-Bucket für die Protokollierung von Bucket A zu Bucket B ändern, werden in der nächsten Stunde einige Protokolle möglicherweise zu Bucket A übermittelt, während andere zu dem neuen Ziel-Bucket B übermittelt werden. In jedem Fall werden die neuen Einstellungen letztendlich ohne weiteres Eingreifen Ihrerseits wirksam.

Themen

Formatierung des Bucket-Zugriffsprotokolls in Amazon Lightsail

Die Zugriffsprotokollierung stellt detaillierte Aufzeichnungen für die Anforderungen bereit, die an einen Bucket im Amazon Lightsail-Objektspeicher-Service gestellt werden. Sie können Zugriffsprotokolle für Sicherheits- und Zugriffsprüfungen verwenden oder mehr über Ihren Kundenstamm erfahren. Dieser Abschnitt beschreibt das Format und andere Details zu Zugriffprotokolldateien. Weitere Informationen zu den Grundlagen der Protokollierung finden Sie unter Bucket-Zugriffsprotokolle.

Die Zugriffsprotokolldateien bestehen aus einer Reihe von durch Zeilenschaltungen voneinander getrennten Protokolldatensätzen. Jeder Protokolldatensatz stellt eine Anforderung dar und besteht aus durch Leerzeichen voneinander getrennter Felder.

Nachfolgend wird ein Beispielprotokoll mit sechs Protokolldatensätzen gezeigt.

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 awsexamplebucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
```

```
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 3E57427F3EXAMPLE
 REST.GET.VERSIONING - "GET /awsexamplebucket1?versioning HTTP/1.1" 200 - 113 - 7 -
 "-" "S3Console/0.4" - s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/
XV/VLi31234= SigV2 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader awsexamplebucket1.s3.us-
west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 awsexamplebucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 891CE47D2EXAMPLE
 REST.GET.LOGGING_STATUS - "GET /awsexamplebucket1?logging HTTP/1.1" 200 - 242
 - 11 - "-" "S3Console/0.4" - 9vKBE6vMhrNiWHZmb2L0mXOcqPGzQOI5XLnCtZNPxev+Hf
+7tpT6sxDwDty4LHBUOZJG96N1234= SigV2 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader
 awsexamplebucket1.s3.us-west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 awsexamplebucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be A1206F460EXAMPLE
 REST.GET.BUCKETPOLICY - "GET /awsexamplebucket1?policy HTTP/1.1" 404
 NoSuchBucketPolicy 297 - 38 - "-" "S3Console/0.4" - BNaBsXZQQDbssi6xMBdBU2sLt
+Yf5kZDmeBUP35sFoKa3sLLeMC78iwEIWxs99CRUrbS4n11234= SigV2 ECDHE-RSA-AES128-GCM-SHA256
 AuthHeader awsexamplebucket1.s3.us-west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 awsexamplebucket1 [06/Feb/2019:00:01:00 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 7B4A0FABBEXAMPLE
 REST.GET.VERSIONING - "GET /awsexamplebucket1?versioning HTTP/1.1" 200 - 113
 - 33 - "-" "S3Console/0.4" - Ke1bUcazaN1jWuUlPJaxF64cQVpUEhoZKEG/hmy/gijN/
I1DeWqDfFvnpybfEseEME/u7ME1234= SigV2 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader
 awsexamplebucket1.s3.us-west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 awsexamplebucket1 [06/Feb/2019:00:01:57 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 DD6CC733AEXAMPLE REST.PUT.OBJECT s3-dg.pdf "PUT /awsexamplebucket1/
s3-dg.pdf HTTP/1.1" 200 - - 4406583 41754 28 "-" "S3Console/0.4" -
 10S62Zv81kBW7BB6SX4XJ48o6kpcl6LPwEoizZQQxJd5qDSCTLX0TgS37kYUBKQW3+bPdrg1234= SigV4
 ECDHE-RSA-AES128-SHA AuthHeader awsexamplebucket1.s3.us-west-1.amazonaws.com TLSV1.1
```

> **Note**
>
> Jedes Protokolldatensatzfeld kann auf – (Bindestrich) gesetzt werden, um anzuzeigen, dass die Daten unbekannt oder nicht verfügbar waren oder dass das Feld auf die Anforderung nicht anwendbar war.

Inhalt

Protokolldatensatzfelder

In der folgenden Liste werden die wichtigsten Protokolldatensatzfelder beschrieben.

Zugangspunkt-ARN (Amazon-Ressourcenname)

Der Amazon-Ressourcenname (ARN) des Zugriffspunkts der Anforderung. Wenn der Zugriffspunkt-ARN fehlerhaft ist oder nicht verwendet wird, enthält das Feld ein „-“. Weitere Informationen zu Zugangspunkten finden Sie unter Verwenden von Zugangspunkten. Weitere Informationen zu ARNs finden Sie im Thema auf Amazon-Ressourcenname (ARN) in der allgemeinen AWS-Referenz.

Beispieleintrag

```
arn:aws:s3:us-east-1:123456789012:accesspoint/example-AP
```

Bucket-Eigentümer

Die kanonische Benutzer-ID des Eigentümer des Quell-Buckets. Die kanonische Benutzer-ID ist eine andere Form der AWS-Konto-ID. Weitere Informationen zur kanonischen Benutzer-ID finden Sie unter AWS-Konto-Kennungen in der Allgemeinen AWS-Referenz. Informationen darüber, wo Sie die kanonische Benutzer-ID für Ihr Konto finden, finden Sie unter Wie Sie die kanonische Benutzer-ID für Ihr AWS-Konto finden.

Beispieleintrag

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Bucket

Der Name des Buckets, für den die Anforderung verarbeitet wurde. Wenn das System eine fehlerhaft aufgebaute Anforderung erhält und den Bucket nicht bestimmen kann, erscheint die Anforderung nicht in einem Zugriffsprotokoll.

Beispieleintrag

```
awsexamplebucket1
```

Time (Zeit)

Die Uhrzeit, zu der die Anforderung empfangen wurde. Diese Datums- und Uhrzeitangaben entsprechen der Zeitzone UTC (Coordinated Universal Time). Das Format unter Verwendung der *strftime ()*-Terminologie, wie folgt: *[%d/%b/%Y:%H:%M:%S %z]*

Beispieleintrag

```
[06/Feb/2019:00:00:38 +0000]
```

Remote-IP

Die offensichtliche Internetadresse des Auftraggebers. Auf dem Weg vorhandene Proxy-Server und Firewalls könnten die tatsächliche Adresse des Computers verbergen, der die Anforderung gestellt hat.

Beispieleintrag

```
192.0.2.3
```

Auftraggeber

Die kanonische Benutzer-ID des Auftraggebers, oder - für nicht authentifizierte Anforderungen. War der Auftraggeber ein IAM-Benutzer, gibt dieses Feld den IAM-Benutzernamen des Auftraggebers zurück, zusammen mit dem AWS-Root-Konto, zu dem der IAM-Benutzer gehört. Diese ID ist dieselbe, die für den Zugriff zu Kontrollzwecken verwendet wird.

Beispieleintrag

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Anforderungs-ID

Eine von Lightsail generierte Zeichenfolge, die jede Anforderung eindeutig identifiziert.

Beispieleintrag

```
3E57427F33A59F07
```

Operation

Die hier aufgeführte Operation ist deklariert al `SOAP.operation`, `REST.HTTP_method.resource_type`, `WEBSITE.HTTP_method.resource_type` oder `BATCH.DELETE.OBJECT`.

Beispieleintrag

```
REST.PUT.OBJECT
```

Key (Schlüssel)

Der "Schlüssel"-Anteil der Anforderung, URL-codiert, oder "-", wenn die Operation keinen Schlüsselparameter entgegennimmt.

Beispieleintrag

```
/photos/2019/08/puppy.jpg
```

Anforderungs-URI

Der Teil der Anforderungs-URI der HTTP-Anforderungsmeldung.

Beispieleintrag

```
"GET /awsexamplebucket1/photos/2019/08/puppy.jpg?x-foo=bar HTTP/1.1"
```

HTTP-Status

Der numerische HTTP-Statuscode der Antwort.

Beispieleintrag

```
200
```

Fehlercode

Der Amazon-S3-Fehlercode oder „-“, wenn kein Fehler aufgetreten ist.

Beispieleintrag

```
NoSuchBucket
```

Gesendete Bytes

Die Anzahl der in der Antwort gesendeten Bytes, ausgenommen HTTP-Protokoll-Overhead, oder "-", falls null.

Beispieleintrag

```
2662992
```

Objektgröße

Die Gesamtgröße des betreffenden Objekts.

Beispieleintrag

```
3462992
```

Gesamtzeit

Die Anzahl der Millisekunden, wie lange die Anforderung aus Perspektive des Buckets unterwegs war. Dieser Wert wird ab der Zeit gemessen, zu der Ihre Anforderung empfangen wurde, bis zu der Zeit, zu der das letzte Byte der Antwort gesendet wurde. Messungen aus der Perspektive des Clients dauern möglicherweise länger aufgrund der Netzwerklatenz.

Beispieleintrag

```
70
```

Umschlagzeit

Die Anzahl der Millisekunden, wie lange Lightsail gebraucht hat, Ihre Anfrage zu verarbeiten. Dieser Wert wird ab der Zeit gemessen, zu der das letzte Byte Ihrer Anforderung empfangen wurde, bis zu der Zeit, zu der das erste Byte der Antwort gesendet wurde.

Beispieleintrag

```
10
```

Referer

Der Wert des HTTP Referrer-Headers, falls vorhanden. HTTP-Benutzeragenten (z. B. Browser) setzen diesen Header normalerweise auf die URL der verlinkenden oder einbettenden Seite, wenn eine Anforderung erfolgt.

Beispieleintrag

```
"http://www.amazon.com/webservices"
```

Benutzer-Agent

Der Wert des HTTP-User-Agent-Headers.

Beispieleintrag

```
"curl/7.15.1"
```

Versions-ID

Die Versions-ID der Anforderung, oder `-`, wenn die Operation keinen `versionId`-Parameter entgegennimmt.

Beispieleintrag

```
3HL4kqtJvjVBH40Nrjfkd
```

Host-ID

Die x-amz-id-2 oder die erweiterte Lightsail-Anforderungs-ID.

Beispieleintrag

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

Signatur-Version

Die Signaturversion, `SigV2` oder `SigV4`, die für die Authentifizierung der Anforderung verwendet wurde, bzw. ein `-` für nicht authentifizierte Anforderungen.

Beispieleintrag

```
SigV2
```

Cipher Suite

Das Secure Sockets Layer(SSL)-Verschlüsselungsverfahren, das für die HTTPS-Anforderung ausgehandelt wurde bzw. ein `-` für HTTP.

Beispieleintrag

```
ECDHE-RSA-AES128-GCM-SHA256
```

Authentifizierungstyp

Die Art der verwendeten Anforderungsauthentifizierung, `AuthHeader` für Authentifizierungsköpfe, `QueryString` für die Anforderungszeichenfolge (vorsignierte URL) oder ein `-` für nicht authentifizierte Anforderungen.

Beispieleintrag

```
AuthHeader
```

Host-Header

Der für die Verbindung mit Lightsail verwendete Endpunkt.

Beispieleintrag

```
s3.us-west-2.amazonaws.com
```

TLS-Version

Die vom Client ausgehandelte Transport Layer Security(TLS)-Version. Einer der folgenden Werte: `TLSv1`, `TLSv1.1`, `TLSv1.2`; oder `-`, wenn TLS nicht verwendet wurde.

Beispieleintrag

```
TLSv1.2
```

Zusätzliche Protokollierung für KopierVorgänge

Eine Kopieroperation umfasst ein `GET` und ein `PUT`. Aus diesem Grund zeichnen wir für eine Kopieroperation zwei Datensätze auf. Der vorherige Abschnitt beschreibt die Felder für den `PUT`-Teil der Operation. Die folgende Liste beschreibt die Felder in dem Datensatz, die sich auf den `GET`-Teil der Kopieroperation beziehen.

Bucket-Eigentümer

Die kanonische Benutzer-ID des Buckets, der das kopierte Objekt speichert. Die kanonische Benutzer-ID ist eine andere Form der AWS-Konto-ID. Weitere Informationen zur kanonischen Benutzer-ID finden Sie unter AWS-Konto-Kennungen in der Allgemeinen AWS-Referenz. Informationen darüber, wo Sie die kanonische Benutzer-ID für Ihr Konto finden, finden Sie unter Wie Sie die kanonische Benutzer-ID für Ihr AWS-Konto finden.

Beispieleintrag

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Bucket

Die Name des Buckets, der das kopierte Objekt speichert.

Beispieleintrag

```
awsexamplebucket1
```

Time (Zeit)

Die Uhrzeit, zu der die Anforderung empfangen wurde. Diese Datums- und Uhrzeitangaben entsprechen der Zeitzone UTC (Coordinated Universal Time). Das Format unter Verwendung der `strftime()`-Terminologie, nämlich: `[%d/%B/%Y:%H:%M:%S %z]`

Beispieleintrag

```
[06/Feb/2019:00:00:38 +0000]
```

Remote-IP

Die offensichtliche Internetadresse des Auftraggebers. Auf dem Weg vorhandene Proxy-Server und Firewalls könnten die tatsächliche Adresse des Computers verbergen, der die Anforderung gestellt hat.

Beispieleintrag

```
192.0.2.3
```

Auftraggeber

Die kanonische Benutzer-ID des Auftraggebers, oder - für nicht authentifizierte Anforderungen. War der Auftraggeber ein IAM-Benutzer, gibt dieses Feld den IAM-Benutzernamen des Auftraggebers zurück, zusammen mit dem AWS-Root-Konto, zu dem der IAM-Benutzer gehört. Diese ID ist dieselbe, die für den Zugriff zu Kontrollzwecken verwendet wird.

Beispieleintrag

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Anforderungs-ID

Eine von Lightsail generierte Zeichenfolge, die jede Anforderung eindeutig identifiziert.

Beispieleintrag

```
3E57427F33A59F07
```

Operation

Die hier aufgeführte Operation ist deklariert al `SOAP.`*`operation`*, `REST.`*`HTTP_method.resource_type`*, `WEBSITE.`*`HTTP_method.resource_type`* oder `BATCH.DELETE.OBJECT`.

Beispieleintrag

```
REST.COPY.OBJECT_GET
```

Key (Schlüssel)

Der "Schlüssel" des kopierten Objekts, oder "-", wenn die Operation keinen Schlüsselparameter entgegennimmt.

Beispieleintrag

```
/photos/2019/08/puppy.jpg
```

Anforderungs-URI

Der Teil der Anforderungs-URI der HTTP-Anforderungsmeldung.

Beispieleintrag

```
"GET /awsexamplebucket1/photos/2019/08/puppy.jpg?x-foo=bar"
```

HTTP-Status

Der numerische HTTP-Statuscode des `GET`-Teils der Kopieroperation.

Beispieleintrag

```
200
```

Fehlercode

Der Amazon-S3-Fehlercodes des GET-Teils des Kopiervorgangs oder -, wenn kein Fehler aufgetreten ist.

Beispieleintrag

```
NoSuchBucket
```

Gesendete Bytes

Die Anzahl der in der Antwort gesendeten Bytes, ausgenommen HTTP-Protokoll-Overhead, oder "-", falls null.

Beispieleintrag

```
2662992
```

Objektgröße

Die Gesamtgröße des betreffenden Objekts.

Beispieleintrag

```
3462992
```

Gesamtzeit

Die Anzahl der Millisekunden, wie lange die Anforderung aus Perspektive des Buckets unterwegs war. Dieser Wert wird ab der Zeit gemessen, zu der Ihre Anforderung empfangen wurde, bis zu der Zeit, zu der das letzte Byte der Antwort gesendet wurde. Messungen aus der Perspektive des Clients dauern möglicherweise länger aufgrund der Netzwerklatenz.

Beispieleintrag

```
70
```

Umschlagzeit

Die Anzahl der Millisekunden, wie lange Lightsail gebraucht hat, Ihre Anfrage zu verarbeiten. Dieser Wert wird ab der Zeit gemessen, zu der das letzte Byte Ihrer Anforderung empfangen wurde, bis zu der Zeit, zu der das erste Byte der Antwort gesendet wurde.

Beispieleintrag

```
10
```

Referer

Der Wert des HTTP Referrer-Headers, falls vorhanden. HTTP-Benutzeragenten (z. B. Browser) setzen diesen Header normalerweise auf die URL der verlinkenden oder einbettenden Seite, wenn eine Anforderung erfolgt.

Beispieleintrag

```
"http://www.amazon.com/webservices"
```

Benutzer-Agent

Der Wert des HTTP-User-Agent-Headers.

Beispieleintrag

```
"curl/7.15.1"
```

Versions-ID

Die Version-ID des kopierten Objekts, oder `-`, wenn der `x-amz-copy-source`-Header keinen `versionId`-Parameter als Teil der Kopierquelle angegeben hat.

Beispieleintrag

```
3HL4kqtJvjVBH40Nrjfkd
```

Host-ID

Die x-amz-id-2 oder die erweiterte Lightsail-Anforderungs-ID.

Beispieleintrag

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

Signatur-Version

Die Signaturversion, `SigV2` oder `SigV4`, die für die Authentifizierung der Anforderung verwendet wurde, bzw. ein `-` für nicht authentifizierte Anforderungen.

Beispieleintrag

```
SigV2
```

Cipher Suite

Das Secure Sockets Layer(SSL)-Verschlüsselungsverfahren, das für die HTTPS-Anforderung ausgehandelt wurde bzw. ein `-` für HTTP.

Beispieleintrag

```
ECDHE-RSA-AES128-GCM-SHA256
```

Authentifizierungstyp

Die Art der verwendeten Anforderungsauthentifizierung, `AuthHeader` für Authentifizierungsköpfe, `QueryString` für die Anforderungszeichenfolge (vorsignierte URL) oder ein `-` für nicht authentifizierte Anforderungen.

Beispieleintrag

```
AuthHeader
```

Host-Header

Der für die Verbindung mit Lightsail verwendete Endpunkt.

Beispieleintrag

```
s3.us-west-2.amazonaws.com
```

TLS-Version

Die vom Client ausgehandelte Transport Layer Security(TLS)-Version. Einer der folgenden Werte: `TLSv1`, `TLSv1.1`, `TLSv1.2`; oder `-`, wenn TLS nicht verwendet wurde.

Beispieleintrag

```
TLSv1.2
```

Benutzerdefinierte Zugriffsprotokollinformationen

Sie können benutzerdefinierte Informationen angeben, die im Zugriffsprotokolldatensatz für eine Anforderung gespeichert werden. Fügen Sie der URL für die Anforderung dazu einen benutzerdefinierten Abfragefolgenkettenparameter hinzu. Lightsail ignoriert Abfrage-Zeichenfolgenparameter, die mit „x-“ beginnen, aber nimmt diese als Teil des `Request-URI`-Felds des Protokolldatensatzes in den Zugriffsprotokoll-Datensatz für die Anfrage auf.

Beispielsweise verhält sich die Anfrage `GET` für `"s3.amazonaws.com/awsexamplebucket1/photos/2019/08/puppy.jpg?x-user=johndoe"` genauso wie die Anfrage für `"s3.amazonaws.com/awsexamplebucket1/photos/2019/08/puppy.jpg"`, abgesehen davon, dass die Zeichenfolge `"x-user=johndoe"` in das Feld `Request-URI` des entsprechenden Protokolldatensatzes eingefügt wird. Diese Funktionalität steht nur auf der REST-Schnittstelle zur Verfügung.

Aspekte zur Programmierung des erweiterbaren Zugriff-Protokollformats

Möglicherweise erweitern wir gelegentlich das Zugriffsprotokoll-Datensatzformat, indem wir am Ende jeder Zeile neue Felder hinzufügen. Daher sollten Sie jeden Code, der Zugriffsprotokolle analysiert, so schreiben, dass er angefügte Felder verarbeiten kann, die er möglicherweise nicht versteht.

Aktivieren der Bucket-Zugriffsprotokollierung in Amazon Lightsail

Die Zugriffsprotokollierung stellt detaillierte Aufzeichnungen für die Anforderungen bereit, die an einen Bucket im Amazon Lightsail-Objektspeicher-Service gestellt werden. Zugriffsprotokolle sind für viele Anwendungen nützlich. Beispielsweise können Zugriffsprotokoll-Informationen bei Sicherheits- und Zugriffsprüfungen nützlich sein. Es kann Ihnen auch dabei helfen, mehr über Ihren Kundenstamm zu erfahren.

Standardmäßig erfasst Lightsail keine Zugriffsprotokolle für Ihre Buckets. Wenn Sie die Protokollierung aktivieren, stellt Lightsail Zugriffsprotokolle für einen Quell-Bucket in einem von

Ihnen ausgewählten Ziel-Bucket bereit. Sowohl der Quell- als auch der Ziel-Bucket müssen sich in derselben AWS-Region befinden und demselben Konto gehören.

Ein Zugriffsprotokollsatz enthält Details über die Anforderungen, die an einen Bucket gestellt werden. Dabei kann es sich um den Anforderungstyp, die in der Anfrage angegebenen Ressourcen sowie Uhrzeit und Datum der Anfrageverarbeitung handeln. In diesem Handbuch zeigen wir Ihnen, wie Sie die Zugriffsprotokollierung für Ihre Buckets mithilfe der Lightsail-API, der AWS Command Line Interface (AWS CLI) oder AWS-SDKs aktivieren oder deaktivieren.

Weitere Informationen zu den Grundlagen der Protokollierung finden Sie unter Bucket-Zugriffsprotokolle.

Inhalt

Kosten für die Zugriffsprotokollierung

Für die Aktivierung der Zugriffsprotokollierung auf einem Bucket fallen keine zusätzlichen Kosten an. Protokolldateien, die das System an einen Bucket überträgt, belegen jedoch Speicherplatz. Sie können die Protokolldateien jederzeit löschen. Wir berechnen keine Datenübertragungskosten für die Übertragung der Protokolldateien, wenn die Datenübertragung des Protokoll-Buckets innerhalb der konfigurierten monatlichen Gebühr liegt.

Die Zugriffsprotokollierung sollte für den Ziel-Bucket nicht aktiviert sein. Sie können Protokolle in jeden Bucket speichern lassen, der sich in der gleichen Region wie der Quell-Bucket befindet, einschließlich des Quell-Buckets selbst. Zur einfacheren Protokollverwaltung empfehlen wir jedoch, Zugriffsprotokolle in einem anderen Bucket zu speichern.

Aktivieren der Zugriffsprotokollierung mithilfe der AWS CLI

Um die Zugriffsprotokollierung für Ihre Buckets zu aktivieren, empfehlen wir Ihnen, in jeder AWS-Region, in der Sie Buckets haben, einen dedizierten Protokollierungs-Bucket zu erstellen. Lassen Sie dann das Zugriffsprotokoll an diesen dedizierten Protokoll-Bucket liefern.

Führen Sie die folgenden Schritte aus, um die Zugriffsprotokollierung mithilfe der AWS CLI zu aktivieren.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail konfigurieren, bevor Sie mit diesem Vorgang fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminalfenster auf Ihrem lokalen Computer.
2. Geben Sie den folgenden Befehl ein, um die Zugriffsprotokollierung zu aktivieren.

```
aws lightsail update-bucket --bucket-name SourceBucketName --access-log-config
 "{\"enabled\": true, \"destination\": \"TargetBucketName\", \"prefix\":
 \"ObjectKeyNamePrefix/\"}"
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *SourceBucketName* – Der Name des Quell-Buckets, für den die Zugriffsprotokolle erstellt werden.
- *targetBucketName* – Der Name des Ziel-Buckets, in dem die Zugriffsprotokolle gespeichert werden.
- *ObjectKeyNamePrefix/* – Das optionale Präfix für Objektschlüsselnamen für die Zugriffsprotokolle. Beachten Sie, dass das Präfix mit einem Schrägstrich (/) enden muss.

Beispiel

```
aws lightsail update-bucket --bucket-name MyExampleBucket --access-log-config
 "{\"enabled\": true, \"destination\": \"MyExampleLogDestinationBucket\", \"prefix
\": \"logs/MyExampleBucket/\"}"
```

Im Beispiel ist *MyExampleBucket* der Quell-Bucket, für den Zugriffsprotokolle erstellt werden, *MyExampleLogDestinationBucket* ist der Ziel-Bucket, in dem die Zugriffsprotokolle gespeichert werden und *logs/MyExampleBucket/* ist das Objektschlüsselnamenspräfix für die Zugriffsprotokolle.

Nach der Ausführung des Befehls sollte ein Ergebnis ähnlich dem folgenden Beispiel angezeigt werden. Der Quell-Bucket wird aktualisiert und die Zugriffsprotokolle sollten beginnen, im Ziel-Bucket zu generieren und gespeichert zu werden.

```
c:\Models>aws lightsail update-bucket --bucket-name MyExampleBucket
--access-log-config "{\"enabled\": true, \"destination\": \"MyExampleLogDestinationBucket\", \"prefix\": \"logs/MyExampleBucket/\"}"

{
    "bucket": {
        "resourceType": "Bucket",
        "accessRules": {
            "getObject": "private",
            "allowPublicOverrides": false
        },
        "arn": "
        "bundleId": "large_1_0",
        "createdAt": "2021-06-29T08:12:39.163000-07:00",
        "url": "
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "name": "
        "supportCode": "
        "tags": [],
        "objectVersioning": "Suspended",
        "ableToUpdateBundle": true,
        "readonlyAccessAccounts": [
            "
        ],
        "state": {
            "code": "OK"
        },
        "accessLogConfig": {
            "enabled": true,
            "destination": "MyExampleLogDestinationBucket"
            "prefix": "logs/MyExampleBucket/"
        }
    },
    "operations": [
        {
            "id": "7ee31ae9-2946-4889-9083-4b0459538162",
            "resourceName": "
            "resourceType": "Bucket",
            "createdAt": "2021-10-22T12:42:11.792000-07:00",
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "
            "operationType": "UpdateBucket",
            "status": "Succeeded",
            "statusChangedAt": "2021-10-22T12:42:11.792000-07:00",
            "errorCode": "",
            "errorDetails": ""
        }
    ]
}
```

Deaktivieren der Zugriffsprotokollierung mithilfe der AWS CLI

Führen Sie die folgenden Schritte aus, um die Zugriffsprotokollierung mithilfe der AWS CLI zu deaktivieren.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail konfigurieren, bevor Sie mit diesem Vorgang fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminalfenster auf Ihrem lokalen Computer.
2. Geben Sie den folgenden Befehl ein, um die Zugriffsprotokollierung zu deaktivieren.

```
aws lightsail update-bucket --bucket-name SourceBucketName --access-log-config
 "{\"enabled\": false}"
```

Ersetzen Sie im Befehl *SourceBucketName* mit dem Namen des Quell-Buckets, für den die Zugriffsprotokollierung deaktiviert werden soll.

Beispiel

```
aws lightsail update-bucket --bucket-name MyExampleBucket --access-log-config
 "{\"enabled\": false}"
```

Nach der Ausführung des Befehls sollte ein Ergebnis ähnlich dem folgenden Beispiel angezeigt werden.

```
>aws lightsail update-bucket --bucket-name MyExampleBucket --access-log-config "{\"enabled\": false}"
{
    "bucket": {
        "resourceType": "Bucket",
        "accessRules": {
            "getObject": "private",
            "allowPublicOverrides": false
        },
        "arn": "
        "bundleId": "large_1_0",
        "createdAt": "2021-06-29T08:12:39.163000-07:00",
        "url": "
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "name": "
        "supportCode": "
        "tags": [],
        "objectVersioning": "Suspended",
        "ableToUpdateBundle": true,
        "readonlyAccessAccounts": [
            "
        ],
        "state": {
            "code": "OK"
        },
        "accessLogConfig": {
            "enabled": false
        }
    },
    "operations": [
        {
            "id": "
            "resourceName": "
            "resourceType": "Bucket",
            "createdAt": "2021-10-22T13:24:36.881000-07:00",
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "
            "operationType": "UpdateBucket",
            "status": "Succeeded",
            "statusChangedAt": "2021-10-22T13:24:36.881000-07:00",
            "errorCode": "",
            "errorDetails": ""
        }
    ]
}
```

Verwenden von Bucket-Zugriffsprotokollen zum Identifizieren von Anforderungen in Amazon Lightsail

In dieser Anleitung zeigen wir Ihnen, wie Sie Anforderungen an einen Bucket mithilfe von Zugriffsprotokollen identifizieren können. Weitere Informationen finden Sie unter Bucketzugriffsprotokolle.

Inhalt

- Abfragen von Zugriffsprotokollen für Anfragen mit Amazon Athena
- Verwenden von Amazon-S3-Zugriffsprotokollen zum Identifizieren von Objektzugriffsanforderungen

Abfragen von Zugriffsprotokollen für Anfragen mit Amazon Athena

Sie können Amazon Athena verwenden, um Anfragen an einen Bucket in Zugriffsprotokollen abzufragen und zu identifizieren.

Lightsail speichert Sugriffsprotokolle als Objekte in einem Lightsail-Bucket. Es ist oft einfacher, ein Tool zu verwenden, mit dem die Protokolle analysiert werden können. Athena unterstützt die Analyse von Objekten und kann zur Abfrage von Zugriffsprotokollen verwendet werden.

Beispiel

Das folgende Beispiel zeigt, wie Sie Bucket-Server-Zugriffsprotokolle in Amazon Athena abfragen können.

> **Note**
>
> Um einen Speicherort in einer Athena-Abfrage anzugeben, müssen Sie den Bucket-Namen des Ziel und das Präfix des Ziels, an das Ihre Protokolle als S3-URI übermittelt werden, wie folgt formatieren: `s3://DOC-EXAMPLE-BUCKET1-logs/prefix/`

1. Öffnen Sie die Athena-Konsole unter https://console.aws.amazon.com/athena/.
2. Führen Sie im Abfrage-Editor einen Befehl wie den folgenden aus.

   ```
   create database bucket_access_logs_db
   ```

   > **Note**
   >
   > Es hat sich bewährt, die Datenbank in der AWS-Region zu erstellen, in der sich der S3-Bucket befindet.

3. Führen Sie im Abfrage-Editor einen Befehl wie den folgenden aus, um in der in Schritt 2 erstellten Datenbank ein Tabellenschema zu erstellen. Die Datentypwerte `STRING` und `BIGINT` sind die Zugriffsprotokolleigenschaften. Sie können diese Eigenschaften in Athena abfragen. Geben Sie für `LOCATION` wie oben erwähnt den Pfad von Bucket und Präfix ein.

```
CREATE EXTERNAL TABLE `s3_access_logs_db.mybucket_logs`(
  `bucketowner` STRING,
  `bucket_name` STRING,
  `requestdatetime` STRING,
  `remoteip` STRING,
  `requester` STRING,
  `requestid` STRING,
  `operation` STRING,
  `key` STRING,
  `request_uri` STRING,
  `httpstatus` STRING,
  `errorcode` STRING,
  `bytessent` BIGINT,
  `objectsize` BIGINT,
  `totaltime` STRING,
  `turnaroundtime` STRING,
  `referrer` STRING,
  `useragent` STRING,
  `versionid` STRING,
  `hostid` STRING,
  `sigv` STRING,
  `ciphersuite` STRING,
  `authtype` STRING,
  `endpoint` STRING,
  `tlsversion` STRING)
ROW FORMAT SERDE
  'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
  'input.regex'='([^ ]*) ([^ ]*) \\[(.*?)\\] ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) (-|[0-9]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 (\"[^\"]*\"|-) ([^ ]*)(?: ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*))?.*$')
STORED AS INPUTFORMAT
  'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
  'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
  's3://doc-example-bucket1-logs/prefix/'
```

4. Wählen Sie im Navigationsbereich unter Database (Datenbank) die Datenbank aus.
5. Wählen Sie unter Tables (Tabellen)neben dem Namen der Tabelle Preview table (Tabellenvorschau) aus.

Im Fensterbereich Results (Ergebnisse) sollten Daten aus den Server-Zugriffsprotokollen angezeigt werden, also `bucketowner`, `bucket`, `requestdatetime` usw. Dies bedeutet, dass die Athena-Tabelle erfolgreich erstellt wurde. Sie können die Bucket-Server-Zugriffsprotokolle jetzt abfragen.

Beispiel – Anzeigen, wer ein Objekt um welche Uhrzeit (Zeitstempel, IP-Adresse und IAM-Benutzer) gelöscht hat

```
SELECT RequestDateTime, RemoteIP, Requester, Key
FROM s3_access_logs_db.mybucket_logs
WHERE key = 'images/picture.jpg' AND operation like '%DELETE%';
```

Beispiel – Anzeigen aller Vorgänge, die von einem IAM-Benutzer ausgeführt wurden

```
SELECT *
FROM s3_access_logs_db.mybucket_logs
WHERE requester='arn:aws:iam::123456789123:user/user_name';
```

Beispiel – Anzeigen aller Vorgänge, die in einem bestimmten Zeitraum für ein Objekt ausgeführt wurden

```
SELECT *
FROM s3_access_logs_db.mybucket_logs
WHERE Key='prefix/images/picture.jpg'
    AND parse_datetime(RequestDateTime,'dd/MMM/yyyy:HH:mm:ss Z')
    BETWEEN parse_datetime('2017-02-18:07:00:00','yyyy-MM-dd:HH:mm:ss')
    AND parse_datetime('2017-02-18:08:00:00','yyyy-MM-dd:HH:mm:ss');
```

Beispiel – Anzeigen der Menge der von einer bestimmten IP-Adresse in einem bestimmten Zeitraum übertragenen Daten

```
SELECT SUM(bytessent) AS uploadTotal,
      SUM(objectsize) AS downloadTotal,
      SUM(bytessent + objectsize) AS Total
FROM s3_access_logs_db.mybucket_logs
WHERE RemoteIP='1.2.3.4'
AND parse_datetime(RequestDateTime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2017-06-01','yyyy-MM-dd')
AND parse_datetime('2017-07-01','yyyy-MM-dd');
```

Verwenden von Amazon-S3-Zugriffsprotokollen zum Identifizieren von Objektzugriffsanforderungen

Sie können Abfragen an Zugriffsprotokolle verwenden, um Objektzugriffsanforderungen für Operationen zu identifizieren, wie etwa GET, PUT und DELETE und weitere Informationen über diese Anforderungen zu erkunden.

Das folgende Amazon-Athena-Abfragebeispiel zeigt, wie alle PUT-Objektanfragen für einen Bucket aus dem Server-Zugriffsprotokoll abgerufen werden.

Beispiel – Anzeigen aller Anforderer, die PUT-Objektanforderungen in einem bestimmten Zeitraum senden

```
SELECT Bucket, Requester, RemoteIP, Key, HTTPStatus, ErrorCode, RequestDateTime
FROM s3_access_logs_db
WHERE Operation='REST.PUT.OBJECT' AND
parse_datetime(RequestDateTime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

Das folgende Amazon Athena-Abfragebeispiel zeigt, wie alle GET-Objektanfragen für Amazon S3 aus dem Server-Zugriffsprotokoll abgerufen werden.

Beispiel – Anzeigen aller Anforderer, die GET-Objektanforderungen in einem bestimmten Zeitraum senden

```
SELECT Bucket, Requester, RemoteIP, Key, HTTPStatus, ErrorCode, RequestDateTime
FROM s3_access_logs_db
WHERE Operation='REST.GET.OBJECT' AND
parse_datetime(RequestDateTime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

Das folgende Amazon Athena-Abfragebeispiel zeigt, wie alle anonymen Anforderungen aus dem Server-Zugriffsprotokoll in Ihre S3-Buckets gelangen.

Beispiel – Anzeigen aller anonymen Anforderer, die in einem bestimmten Zeitraum Anforderungen an einen Bucket richten

```
SELECT Bucket, Requester, RemoteIP, Key, HTTPStatus, ErrorCode, RequestDateTime
FROM s3_access_logs_db.mybucket_logs
WHERE Requester IS NULL AND
parse_datetime(RequestDateTime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

Note

- Sie können den Datumsbereich an Ihre Anforderungen anpassen.
- Diese Abfragebeispiele können auch für die Sicherheitsüberwachung nützlich sein. Sie können die Ergebnisse auf `PutObject`- oder `GetObject`-Aufrufe von unerwarteten oder nicht autorisierten IP-Adressen/Anforderern und zum Aufdecken anonymer Anforderungen an Ihre Buckets prüfen.
- Diese Abfrage ruft nur Informationen von der Zeit ab, zu der die Protokollierung aktiviert wurde.

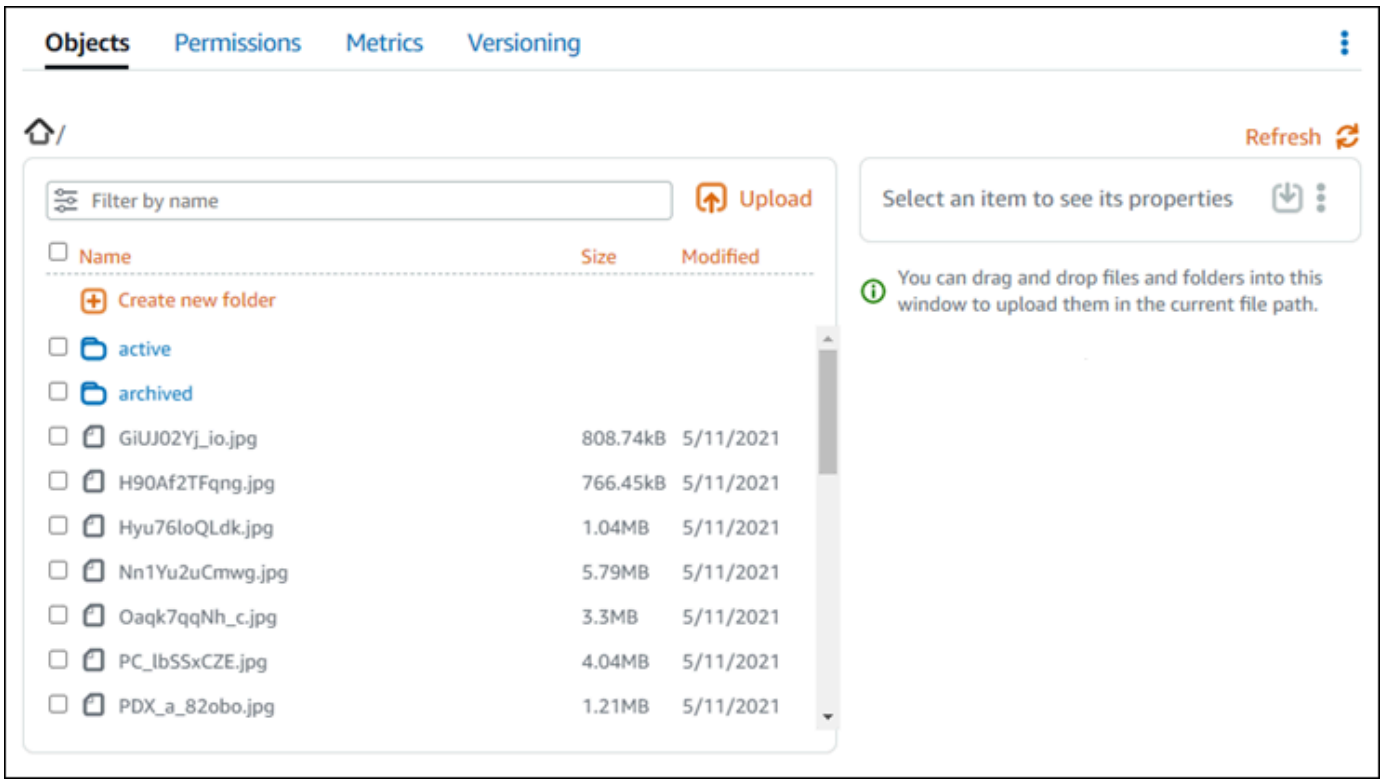
Bucket-Objekte in Amazon Lightsail

Sie können alle Objekte, die in Ihrem Bucket gespeichert sind, im Amazon Lightsail-Objektspeicherdienst mithilfe der Lightsail-Konsole anzeigen. Sie können auch die AWS Command Line Interface (AWS CLI) und AWS-SDKs verwenden, um Objektschlüssel in Ihrem Bucket aufzulisten. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

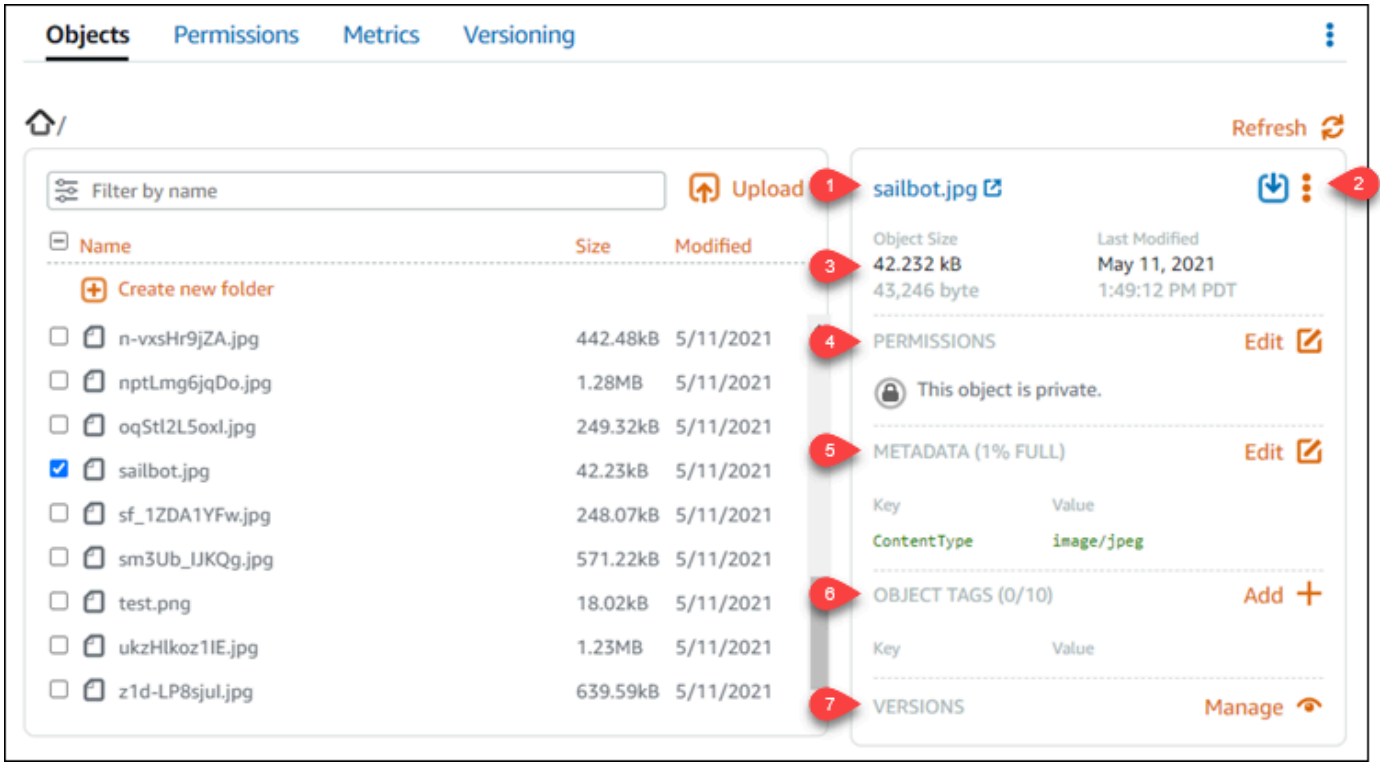
Filtern von Objekten mit der Lightsail-Konsole

Vervollständigen Sie das folgende Verfahren, um Objekte, die in einem Bucket gespeichert sind, mit der Lightsail-Konsole anzuzeigen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen der Datenbank, für die Sie die Protokolle anzeigen möchten.
4. Der Bereich Browser Objekte in Registerkarte „Objekte“ zeigt die Objekte und Ordner an, die in Ihrem Bucket gespeichert sind.



5. Navigieren Sie zum Speicherort des Objekts, für das Sie Eigenschaften anzeigen möchten.
6. Fügen Sie ein Häkchen neben dem Objekt hinzu, für das Sie Eigenschaften anzeigen möchten.
7. Der Bereich Objekteigenschaften rechts auf der Seite zeigt Ihnen Informationen über das Objekt an.



Die angezeigten Informationen umfassen:

1. Links zum Anzeigen und Herunterladen des Objekts.
2. Aktionen-Menü (⋮), um das Objekt zu kopieren oder zu löschen. Weitere Informationen über das Kopieren und Löschen von Objekten finden Sie unter Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail und Löschen von Objekten in einem Bucket.
3. Objektgröße und Zeitstempel zuletzt geändert.
4. Die Zugriffsberechtigung für das einzelne Objekt, das privat oder öffentlich sein kann (schreibgeschützt). Weitere Informationen zu Objektberechtigungen finden Sie unter Bucket-Berechtigungen.
5. Die Metadaten des Objekts. Der Inhaltstyp (`ContentType`) sind die einzigen Metadaten, die vom Lightsail-Objektspeicherdienst zu diesem Zeitpunkt.
6. Die Objektschlüssel-Wert-Tags. Weitere Informationen finden Sie unter Markieren von Objekten in einem Bucket.
7. Die Option zum Verwalten gespeicherter Versionen des Objekts. Weitere Informationen finden Sie unter Aktivieren und Aussetzen der Bucket-Objekt-Versionsverwaltung.

> **Note**
>
> Wenn Sie mehrere Objekte auswählen, zeigt der Bereich Objekteigenschaften nur die Gesamtgröße der ausgewählten Objekte an.

Anzeigen von Objekten mit der AWS CLI

Vervollständigen Sie das folgende Verfahren, um Objekte in einem Bucket mithilfe der AWS Command Line Interface (AWS CLI) zu filtern. Führen Sie dazu den Befehl `list-objects-v2` aus. Weitere Informationen finden Sie unter list-objects-v2 in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS Command Line Interface für die Arbeit mit Amazon Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie einen der folgenden Befehle ein.

   - Geben Sie den folgenden Befehl ein, um alle Objektschlüssel in Ihrem Bucket aufzulisten.

     ```
     aws s3api list-objects-v2 --bucket BucketName --query "Contents[].{Key: Key,
      Size: Size}"
     ```

     Ersetzen Sie im Befehl *BucketName* mit dem Namen des Buckets, für das Sie alle Objekte aufführen möchten.

   - Geben Sie den folgenden Befehl ein, um Objekte aufzulisten, die mit einem bestimmten Objektschlüsselnamen-Präfix beginnen.

     ```
     aws s3api list-objects-v2 --bucket BucketName --prefix ObjectKeyNamePrefix --
     query "Contents[].{Key: Key, Size: Size}"
     ```

     Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *BucketName* – Der Name des Buckets, für das Sie alle Objekte aufführen möchten.
- *ObjectKeyNamePrefix* – Ein Objektschlüsselnamenpräfix, um die Antwort auf Schlüssel zu beschränken, die mit dem angegebenen Präfix beginnen.

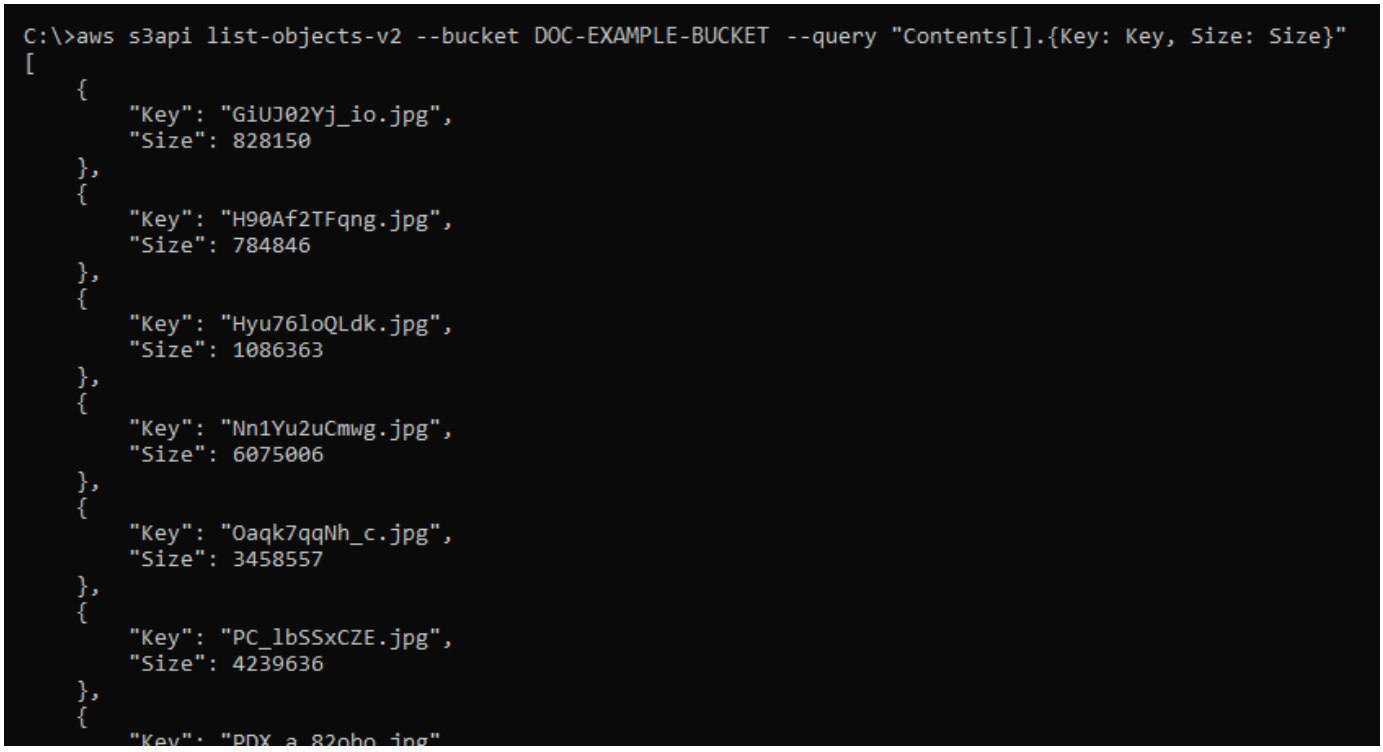
> **Note**
>
> Dieser Befehl verwendet die `--query`-Parameter, um die Antwort der `list-objects-v2`-Anforderung auf den Schlüsselwert und die Größe jedes Objekts zu filtern.

Beispiele:

Alle Objektversionen in einem Bucket auflisten:

```
aws s3api list-objects-v2 --bucket DOC-EXAMPLE-BUCKET --query "Contents[].{Key:
 Key, Size: Size}"
```

Sie sollten für den vorherigen Befehl ein Ergebnis ähnlich dem folgenden Beispiel erhalten.



Auflisten von Objektschlüsseln, die mit dem `archived/`Präfix Objektschlüsselnamenpräfix gestartet werden:

```
aws s3api list-objects-v2 --bucket DOC-EXAMPLE-BUCKET --prefix archived/ --query
 "Contents[].{Key: Key, Size: Size}"
```

Sie sollten für den vorherigen Befehl ein Ergebnis ähnlich dem folgenden Beispiel erhalten.

```
C:\>aws s3api list-objects-v2  --bucket DOC-EXAMPLE-BUCKET --prefix archived/ --query "Contents[].{Key: Key, Size: Size}"
[
    {
        "Key": "archived/",
        "Size": 0
    },
    {
        "Key": "archived/1_CMoFsPfso.jpg",
        "Size": 2561865
    },
    {
        "Key": "archived/3y1zF4hIPCg.jpg",
        "Size": 6404907
    },
    {
        "Key": "archived/5IHz5WhosQE.jpg",
        "Size": 2377975
    },
    {
        "Key": "archived/sailbot.jpg",
        "Size": 43246
    }
]
```

Verwalten von Buckets und Objekten

Dies sind die allgemeinen Schritte zum Verwalten Ihres Lightsail-Objektspeicher-Buckets:

1. Weitere Informationen über Buckets und Objekte im Amazon Lightsail-Objektspeicherservice. Weitere Informationen zu Buckets finden Sie unter Objektspeicher in Amazon Lightsail.
2. Erfahren Sie mehr über die Namen, die Sie Ihren Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Namensregeln für Buckets in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherservice, indem Sie einen Bucket erstellen. Weitere Informationen finden Sie unter Buckets erstellen in Amazon Lightsail.
4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren.

Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Lightsail-Objektspeicher und Bucket-Berechtigungen in Amazon Lightsail verstehen.

Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

- Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail
- Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail
- Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
- Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
- Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail
- Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail

5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherservice
   - Zugriffsprotokollierungsformat für Buckets im Amazon Lightsail-Objektspeicher-Service
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicher-Service
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail, um Anforderungen zu identifizieren
6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gewährt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets in Amazon Lightsail.
7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unterGrundlegendes zu Objektschlüsselnamen inAmazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Hochladen einer Datei in einen Bucket in Amazon Lightsail
   - Hochladen von Dateien in Buckets in Amazon Lightsail mit mehrteiligem Upload
   - Anzeigen von Objekten in einem Bucket in Amazon Lightsail
   - Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
   - Objekte von einem Bucket in Amazon Lightsail herunterladen

- Filtern von Objekten in einem Bucket in Amazon Lightsail
- Markieren von Objekten in einem Bucket in Amazon Lightsail
- Löschen von Objekten in einem Bucket in Amazon Lightsail

9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.
10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.
11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.
12. Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen in Amazon Lightsail.
13. Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Tarifs Ihres Buckets in Amazon Lightsail.
14. Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.
    - Tutorial: Verbinden einer WordPress-Instance mit einem Amazon Lightsail-Bucket
    - Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Lightsail-Netzwerkverteilung für die Bereitstellung von Inhalten
15. Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

Themen

- Bucket-Objekte nach Amazon Lightsail kopieren und verschieben
- Bucket-Objekte in Amazon Lightsail löschen
- Objekte von einem Bucket in Amazon Lightsail herunterladen
- Bucket-Objekte in Amazon Lightsail filtern
- Objekt-Versionsverwaltung in Amazon Lightsail aktivieren und aussetzen
- Wiederherstellen früherer Versionen von Bucket-Objekten in Amazon Lightsail

- Bucket-Objekte in Amazon Lightsail taggen

Bucket-Objekte nach Amazon Lightsail kopieren und verschieben

Sie können Objekte kopieren, die bereits in Ihrem Bucket im Amazon Lightsail-Objektspeicherdienst gespeichert sind. In dieser Anleitung zeigen wir Ihnen, wie Sie Objekte mittels Lightsail-Konsole und AWS Command Line Interface (AWS CLI) kopieren. Kopieren Sie Objekte in Ihrem Bucket, um doppelte Kopien von Objekten zu erstellen, Objekte umzubenennen oder Objekte über Lightsail-Standorte (z. B. Verschieben von Objekten aus einer AWS-Region zu einer anderen, in der Lightsail verfügbar ist). Sie können Objekte nur mithilfe der AWS-APIs, AWS-SDKs und AWS Command Line Interface (AWS CLI) standortübergreifend kopieren.

Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Einschränkungen beim Kopieren von Objekten

Sie können eine Kopie eines Objekts mit einer Größe von bis zu 2 GB mit derLightsailKonsole erstellen. Sie können eine Kopie eines Objekts mit einer Größe von bis zu 5 GB mit einer einzigen Kopieraktion von Objekten mithilfe der AWS Command Line Interface (AWS CLI), AWS-APIs und AWS-SDKs erstellen. Um ein Objekt zu kopieren, das größer als 5 GB ist, müssen Sie die mehrteilige Uploadaktion der AWS CLI, AWS-APIs und AWS-SDKs verwenden. Weitere Informationen finden Sie unter Hochladen von Dateien in einen Bucket mithilfe von mehrteiligen Uploads.

Kopieren von Objekten mithilfe derLightsail Konsole

Vervollständigen Sie das folgende Verfahren, um ein Objekt zu kopieren, das in einem Bucket gespeichert ist, mithilfe derLightsail Konsole. Um ein Objekt in einem Bucket zu verschieben, sollten Sie es an die neue Position kopieren und das ursprüngliche Objekt löschen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen des Buckets aus, für den Sie ein Objekt kopieren möchten.
4. In der Registerkarte Objekte verwenden SieObjekbrowser-Fenster, um zum Speicherort des Objekts zu navigieren, das Sie kopieren möchten.
5. Fügen Sie ein Häkchen neben dem Objekt hinzu, das Sie kopieren möchten.
6. Im Fenster Objektinformationen das Menü Aktionen (⋮) und dann Kopieren nach auswählen.

7. Im angezeigten Fenster Ziel auswählen zum Speicherort im Bucket navigieren, an dem Sie das ausgewählte Objekt kopieren möchten. Sie können auch einen neuen Pfad erstellen, indem Sie Ordnernamen im Textfeld Zielpfadeingeben.
8. Klicken Sie aufKopieren, um das Objekt in das ausgewählte oder angegebene Ziel zu kopieren. Andernfalls wählen Sie Nein, abbrechen.

   Die Meldung Kopieren abgeschlossen wird angezeigt, wenn das Objekt erfolgreich kopiert wurde. Sie sollten das ursprüngliche Objekt löschen, wenn Sie beabsichtigen, das Objekt zu verschieben. Weitere Informationen hierzu finden Sie unter Bucketobjekte löschen.

Kopieren von Objekten mithilfe von AWS CLI

Vervollständigen Sie das folgende Verfahren, um Objekte in einen Bucket mithilfe der AWS Command Line Interface (AWS CLI) zu kopieren. Führen Sie dazu den Befehl `copy-object` aus. Weitere Informationen finden Sie unter copy-object in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um ein Objekt in Ihrem Bucket zu kopieren.

   ```
   aws s3api copy-object --copy-source SourceBucketNameAndObjectKey --
   key DestinationObjectKey --bucket DestinationBucketName --acl bucket-owner-full-
   control
   ```

   Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

   - *SourceBucketNameAndObjectKey*- Der Name des Buckets, in dem das Quellobjekt derzeit vorhanden ist, und der vollständige Objektschlüssel des zu kopierenden Objekts. Zum Beispiel, um das Objekt `images/sailbot.jpg` aus einem Bucket `DOC-EXAMPLE-BUCKET` zu kopieren, geben Sie `DOC-EXAMPLE-BUCKET/images/sailbot.jpg` an.
   - *DestinationObjectKey*- Der vollständige Objektschlüssel der neuen Objektkopie.

- *DestinationBucket*- Der Name des Zielbuckets.

Beispiele:

- Kopieren eines Objekts aus einem Bucket in denselben Bucket:

```
aws s3api copy-object --copy-source DOC-EXAMPLE-BUCKET/images/sailbot.jpg --
key media/sailbot.jpg --bucket DOC-EXAMPLE-BUCKET --acl bucket-owner-full-control
```

- Kopieren eines Objekts von einem Bucket in einen anderen Bucket:

```
aws s3api copy-object --copy-source DOC-EXAMPLE-BUCKET-1/images/sailbot.jpg --
key images/sailbot.jpg --bucket DOC-EXAMPLE-BUCKET-2 --acl bucket-owner-full-
control
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

```
C:\>aws s3api copy-object --copy-source DOC-EXAMPLE-BUCKET/images/sailbot.jpg --key images/archived/sailbot.jpg --bucket DOC-EXAMPLE-BUCKET
{
    "ServerSideEncryption": "AES256",
    "CopyObjectResult": {
        "ETag": "\"694d34example91d92d64f342aa234c3\"",
        "LastModified": "2021-05-10T05:35:42+00:00"
    }
}
```

Verwalten von Buckets und Objekten

Dies sind die allgemeinen Schritte zum Verwalten Ihres Lightsail-Objektspeicher-Buckets:

1. Weitere Informationen über Buckets und Objekte im Amazon Lightsail-Objektspeicherservice. Weitere Informationen zu Buckets finden Sie unter Objektspeicher in Amazon Lightsail.
2. Erfahren Sie mehr über die Namen, die Sie Ihren Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Namensregeln für Buckets in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherservice, indem Sie einen Bucket erstellen. Weitere Informationen finden Sie unter Buckets erstellen in Amazon Lightsail.
4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren.

Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Lightsail-Objektspeicher und Bucket-Berechtigungen in Amazon Lightsail verstehen.

Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

- Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail
- Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail
- Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
- Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
- Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail
- Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail

5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherservice
   - Zugriffsprotokollierungsformat für Buckets im Amazon Lightsail-Objektspeicher-Service
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicher-Service
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail, um Anforderungen zu identifizieren
6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gewährt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets in Amazon Lightsail.
7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unterGrundlegendes zu Objektschlüsselnamen inAmazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Hochladen einer Datei in einen Bucket in Amazon Lightsail
   - Hochladen von Dateien in Buckets in Amazon Lightsail mit mehrteiligem Upload
   - Anzeigen von Objekten in einem Bucket in Amazon Lightsail
   - Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
   - Objekte von einem Bucket in Amazon Lightsail herunterladen

- Filtern von Objekten in einem Bucket in Amazon Lightsail
- Markieren von Objekten in einem Bucket in Amazon Lightsail
- Löschen von Objekten in einem Bucket in Amazon Lightsail

9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.
10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.
11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.
12. Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen in Amazon Lightsail.
13. Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Tarifs Ihres Buckets in Amazon Lightsail.
14. Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.
    - Tutorial: Verbinden einer WordPress-Instance mit einem Amazon Lightsail-Bucket
    - Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Lightsail-Netzwerkverteilung für die Bereitstellung von Inhalten
15. Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

Bucket-Objekte in Amazon Lightsail löschen

Sie können Objekte aus Ihrem Bucket imAmazon LightsailObjektspeicherdienst löschen. Löschen Sie Objekte, die Sie nicht mehr benötigen, um Speicherplatz freizugeben. Wenn Sie beispielsweise Protokolldateien sammeln, sollten Sie sie unbedingt löschen, wenn Sie sie nicht mehr brauchen.

Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Inhalt

Löschen von Objekten aus einem versionsfähigen Bucket

Wenn Ihr Bucket versionsfähig ist, kann es innerhalb des Buckets mehrere Versionen desselben Objekts geben. Sie können jede beliebige Version eines Objekts mit der Lightsail-Konsole, AWS CLI, AWS-APIs oder AWS-SDKS löschen. Sie sollten jedoch die folgenden Optionen in Betracht ziehen.

Löschen von Objekten und Objektversionen mithilfe der Lightsail-Konsole

Wenn Sie die aktuelle Version eines Objekts imBrowserfenster Objekteder RegisterkarteObjekte in der Lightsail-Konsole löschen, werden dadurch auch alle vorherigen Versionen des Objekts gelöscht. Um eine bestimmte Objektversion zu löschen, müssen Sie dies im Fenster Verwalten von Versionen vornehmen. Wenn Sie das Fenster Verwalten von Versionen verwenden, um die aktuelle Version eines Objekts zu löschen, dann wird die neueste vorherige Version als aktuelle Version wiederhergestellt. Weitere Informationen finden Sie unter Löschen von Objektversionen mithilfe der Lightsail-Konsole weiter unten in diesem Leitfaden.

Löschen von Objekten und Objektversionen mithilfe des Lightsail-API, AWS CLI oder AWS-SDKs

Um ein einzelnes Objekt und alle seine gespeicherten Versionen zu löschen, geben Sie nur den Objektschlüssel in der Löschanforderung an. Um eine bestimmte Objektversion zu löschen, geben Sie beides an, den Objektschlüssel und die Version-ID. Weitere Informationen finden Sie unter Löschen eines einzelnen Objekts oder von Objektversionen mithilfe der AWS CLI weiter unten in diesem Leitfaden.

Löschen Sie Objekte mithilfe der Lightsail-Konsole

Vervollständigen Sie das folgende Verfahren, um ein Objekt einschließlich der gespeicherten vorherigen Versionen mithilfe der Lightsail-Konsole zu löschen. Sie können jeweils nur ein Objekt mithilfe der Lightsail-Konsole löschen. Verwenden Sie AWS CLI, um mehrere Objekte auf einmal zu löschen. Weitere Informationen finden Sie unter Löschen mehrerer Objekte oder von Objektversionen mithilfe der AWS CLI weiter unten in diesem Leitfaden.

1. Melden Sie sich an der Lightsail-Konsole an.

2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen des Buckets aus, für den Sie Objekte löschen möchten.
4. Verwenden des Fensters Browser Objekte in der Registerkarte Objekte, um zu dem Speicherort des Objekts zu navigieren, das Sie löschen möchten.
5. Fügen Sie ein Häkchen neben dem Objekt hinzu, das Sie löschen möchten.
6. Im Fenster Objektinformationen wählen Sie die Aktion (⋮) Menü, und dann Löschen aus.
7. Bestätigen Sie im angezeigten Bestätigungsfenster, dass Sie das Objekt dauerhaft löschen möchten, indem SieJa, löschen auswählen.

   Wenn Sie das einzige Objekt im Ordner löschen, in dem Sie sich befinden, wird dadurch auch der Ordner gelöscht. Dies geschieht, weil der Ordner Teil des Objektschlüsselnamens ist und das Löschen des Objekts auch die vorhergehenden Ordner löscht, wenn keine anderen Objekte im Bucket dasselbe Objektschlüsselpräfix teilen. Weitere Informationen finden Sie unter Schlüsselnamen für Objektspeicher-Buckets.

Löschen von Objektversionen mithilfe der Lightsail-Konsole

Vervollständigen Sie das folgende Verfahren, um gespeicherte Versionen eines Objekts zu löschen. Dies ist nur für versionsfähige Buckets möglich. Weitere Informationen finden Sie unter Aktivieren und Aussetzen der Bucket-Objekt-Versionsverwaltung.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen des Buckets aus, für den Sie Objekte löschen möchten.
4. Verwenden des Fensters Browser Objekte um zu dem Speicherort des Objekts zu navigieren, das Sie löschen möchten.
5. Fügen Sie ein Häkchen neben dem Objekt hinzu, für das Sie gespeicherten früheren Versionen löschen möchten.
6. Wählen Sie Verwaltenim Abschnitt Versionen im Fenster Objektinformationen, und dann Verwalten.
7. Im Fenster Verwalten gespeicherter Objektversionen, das angezeigt wird, fügen Sie ein Häkchen neben den Versionen des Objekts hinzu, das Sie löschen möchten.

   Sie können auch wählen, die aktuelle Version eines Objekts zu löschen.
8. Wählen Sie Ausgewählte löschen, um die ausgewählten Versionen zu löschen.

Wenn Sie löschen:

- Die aktuelle Version eines Objekts - Die neueste vorherige Version des Objekts wird als aktuelle Version wiederhergestellt.
- Die einzige Version eines Objekts - Das Objekt wird aus dem Bucket gelöscht. Wenn die gelöschte Version das einzige Objekt im aktuellen Ordner ist, wird der Ordner ebenfalls gelöscht. Dies geschieht, weil der Ordner Teil des Objektschlüsselnamens ist und das Löschen des Objekts auch die vorhergehenden Ordner löscht, wenn keine anderen Objekte im Bucket dasselbe Objektschlüsselpräfix teilen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen der Bucket-Objekt-Versionsverwaltung.

Löschen eines einzelnen Objekts oder Objektversion mithilfe der AWS CLI

Vervollständigen Sie das folgende Verfahren, um ein einzelnes Objekt oder eine Objektversion in Ihrem Bucket mithilfe der AWS Command Line Interface (AWS CLI) zu löschen. Führen Sie dazu den Befehl `delete-object` aus. Weitere Informationen finden Sie unter delete-object in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS Command Line Interface für die Arbeit mit Amazon Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um ein Objekt oder eine Objektversion in Ihrem Bucket zu löschen.

   So löschen Sie ein Objekt:

   ```
   aws s3api delete-object --bucket BucketName --key ObjectKey
   ```

   Löschen einer Objektversion:

> **Note**
>
> Das Löschen von Objektversionen ist nur für versionsfähige Buckets möglich. Weitere Informationen finden Sie unter Aktivieren und Aussetzen der Bucket-Objekt-Versionsverwaltung.

```
aws s3api delete-object --bucket BucketName --key ObjectKey --version-id VersionID
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *Bucket-Name* - Der Namen des Buckets, aus dem Sie ein Objekt löschen möchten.
- *Objektschlüssel* - Der vollständige Objektschlüssel des Objekts, das Sie löschen möchten.
- *VersionId*- Die ID der Objektversion, die Sie löschen möchten.

Beispiele:

Löschen eines Objekts:

```
aws s3api delete-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg
```

Löschen einer Objektversion:

```
aws s3api delete-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg --
version-id YF0YMBlUvexampleO07l2vJi9hRz4ujX
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

```
C:\Users\latino>aws s3api delete-object --bucket DOC-EXAMPLE-BUCKET  --key  images/sailbot.jpg  --version-id YF0YMBlUvexampleO07l2vJi9hRz4ujX
{
    "VersionId": "YF0YMBexampleY7PO07l2vJi9hRz4ujX"
}
```

Löschen mehrerer Objekte oder Objektversionen mithilfe der AWS CLI

Vervollständigen Sie das folgende Verfahren, um mehrere Objekte in Ihrem Bucket mithilfe der AWS Command Line Interface (AWS CLI) zu löschen. Führen Sie dazu den Befehl `delete-objects` aus. Weitere Informationen finden Sie unter delete-objects in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS Command Line Interface für die Arbeit mit Amazon Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um mehrere Objekte oder mehrere Objektversionen in Ihrem Bucket zu löschen.

```
aws s3api delete-objects --bucket BucketName --delete file://LocalDirectory
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *Bucket-Name* - Der Namen des Buckets, aus dem Sie mehrere Objekte oder Objektversionen löschen möchten.
- *LocalDirectory* – Der Verzeichnispfad auf Ihrem Computer des .json-Dokuments, der die zu löschenden Objekte oder Versionen angibt. Das .json-Dokument kann wie folgt formatiert werden.

  Um Objekte zu löschen, geben Sie den folgenden Text in die .json-Datei ein und ersetzen*Objektschlüssel* mit dem Objektschlüssel der Objekte, die Sie löschen möchten.

```
{
  "Objects": [
    {
      "Key": "ObjectKey1"
    },
    {
      "Key": "ObjectKey2"
    }
  ],
  "Quiet": false
}
```

  Um Objektversionen zu löschen, geben Sie den folgenden Text in die .json-Datei ein. Ersetzen Sie*Objektschlüssel*und*VersionId* mit dem Objektschlüssel und den IDs der Objektversionen, die Sie löschen möchten.

> **Note**
>
> Das Löschen von Objektversionen ist nur für versionsfähige Buckets möglich. Weitere Informationen finden Sie unter Aktivieren und Aussetzen der Bucket-Objekt-Versionsverwaltung.

```
{
  "Objects": [
    {
      "Key": "ObjectKey1",
      "VersionId": "VersionID1"
    },
    {
      "Key": "ObjectKey2",
      "VersionId": "VersionID2"
    }
  ],
  "Quiet": false
}
```

Beispiele:

- Auf einem Linux- oder Unix-Computer:

```
aws s3api delete-objects --bucket DOC-EXAMPLE-BUCKET --delete file://home/user/
Documents/delete-objects.json
```

- Auf einem Windows-Computer:

```
aws s3api delete-objects --bucket DOC-EXAMPLE-BUCKET --delete file://C:\Users
\user\Documents\delete-objects.json
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

```
C:\>aws s3api delete-objects --bucket DOC-EXAMPLE-BUCKET  --delete file://C:\Users\user\Documents\delete-objects.json
{
    "Deleted": [
        {
            "Key": "images/sailbot.jpg",
            "VersionId": "26sqexampleztRiT6TsGhMMz0FxQAEw."
        },
        {
            "Key": "images/sailbot.jpg",
            "VersionId": "QwDrexampleDJxJtZC1CrExbpNlEC5O4"
        }
    ]
}
```

Verwalten von Buckets und Objekten

Dies sind die allgemeinen Schritte zum Verwalten Ihres Lightsail-Objektspeicher-Buckets:

1. Weitere Informationen über Buckets und Objekte im Amazon Lightsail-Objektspeicherservice. Weitere Informationen zu Buckets finden Sie unter Objektspeicher in Amazon Lightsail.
2. Erfahren Sie mehr über die Namen, die Sie Ihren Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Namensregeln für Buckets in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherservice, indem Sie einen Bucket erstellen. Weitere Informationen finden Sie unter Buckets erstellen in Amazon Lightsail.
4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Lightsail-Objektspeicher und Bucket-Berechtigungen in Amazon Lightsail verstehen.

   Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

   - Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail
   - Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail
   - Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
   - Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
   - Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail
   - Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail

5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherservice
   - Zugriffsprotokollierungsformat für Buckets im Amazon Lightsail-Objektspeicher-Service
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicher-Service
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail, um Anforderungen zu identifizieren
6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gewährt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets in Amazon Lightsail.
7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unterGrundlegendes zu Objektschlüsselnamen inAmazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Hochladen einer Datei in einen Bucket in Amazon Lightsail
   - Hochladen von Dateien in Buckets in Amazon Lightsail mit mehrteiligem Upload
   - Anzeigen von Objekten in einem Bucket in Amazon Lightsail
   - Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
   - Objekte von einem Bucket in Amazon Lightsail herunterladen
   - Filtern von Objekten in einem Bucket in Amazon Lightsail
   - Markieren von Objekten in einem Bucket in Amazon Lightsail
   - Löschen von Objekten in einem Bucket in Amazon Lightsail
9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.
10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.
11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.

12 Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen in Amazon Lightsail.

13 Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Tarifs Ihres Buckets in Amazon Lightsail.

14 Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.

- Tutorial: Verbinden einer WordPress-Instance mit einem Amazon Lightsail-Bucket
- Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Lightsail-Netzwerkverteilung für die Bereitstellung von Inhalten

15 Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

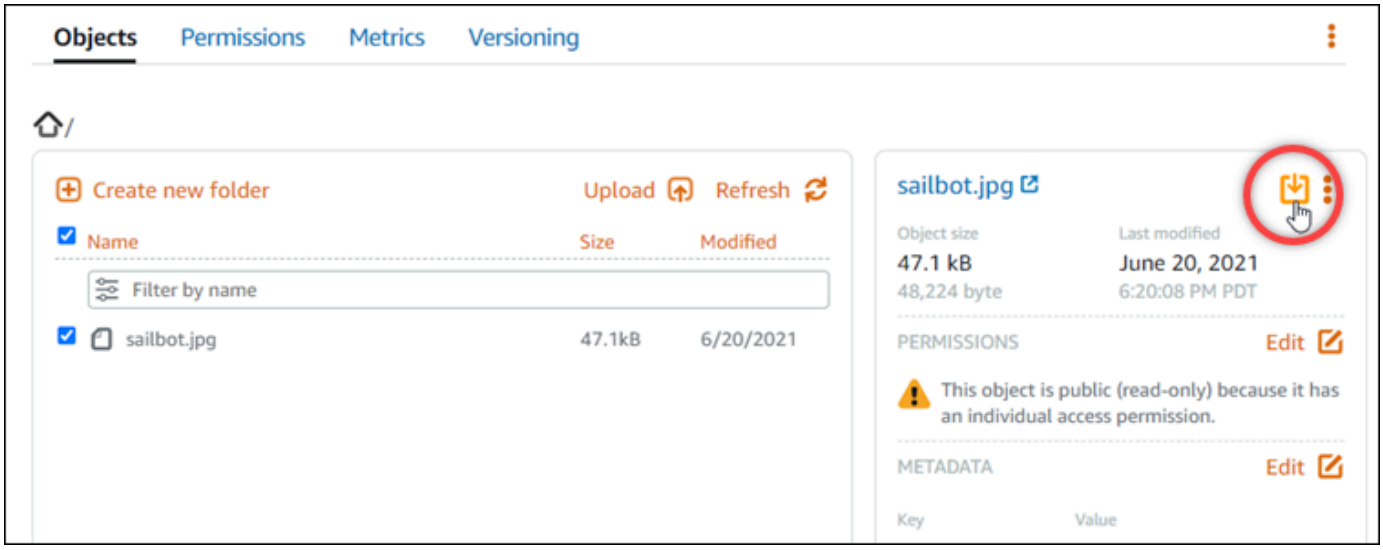
Objekte von einem Bucket in Amazon Lightsail herunterladen

Sie können Objekte aus Buckets herunterladen, auf die Sie Zugriff haben oder die öffentlich sind (schreibgeschützt) imAmazon Lightsail Objektspeicherdienst. Sie können jeweils ein einzelnes Objekt über die Lightsail-Konsole herunterladen. Wenn Sie mehrere Objekte herunterladen möchten, verwenden Sie die AWS Command Line Interface (AWS CLI), AWS-SDKs oder die REST-API.
In diesem Leitfaden zeigen wir Ihnen, wie Sie Objekte mit derLightsail-Konsole undAWS CLI herunterladen. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Herunterladen von Objekten mithilfe der Lightsail-Konsole

Vervollständigen Sie das folgende Verfahren, um Objekte aus einem Bucket mit derLightsail-Konsole herunterzuladen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Name des Buckets, aus dem Sie eine Datei herunteladen möchten.
4. Verwenden Sie in der Registerkarte Objekte, das Fenster Browserobjekte, um zu dem Speicherort des Objekts zu navigieren, das Sie herunterladen möchten.
5. Fügen Sie ein Häkchen neben dem Objekt hinzu, das Sie herunterladen möchten.
6. Wählen Sie im FenterObjektinformationen das Symbol zum Herunterladen.



Abhängig von der Konfiguration Ihres Browsers wird die ausgewählte Datei entweder auf der Seite angezeigt oder auf Ihren Computer heruntergeladen. Wenn die Datei auf der Seite angezeigt wird, können Sie mit der rechten Maustaste darauf klicken undSpeichern als auswählen, um sie auf Ihrem Computer zu speichern.

Herunterladen von Objekten mithilfe der AWS CLI

Vervollständigen Sie das folgende Verfahren, um Objekte aus einem Bucket mit der AWS Command Line Interface (AWS CLI) herunterzuladen. Führen Sie dazu den Befehl `get-object` aus. Weitere Informationen finden Sie unter get-object in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS Command Line Interface für die Arbeit mit Amazon Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um ein Objekt aus Ihrem Bucket herunterzuladen.

```
aws s3api get-object --bucket BucketName --key ObjectKey LocalFilePath
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *Bucket-Name* - Der Namen des Buckets, aus dem Sie ein Objekt herunterladen möchten.
- *Objektschlüssel* - Der vollständige Objektschlüssel des Objekts, das Sie herunterladen möchten.
- *LocalFilePath*- Der vollständige Dateipfad auf Ihrem Computer, auf dem Sie die heruntergeladene Datei speichern möchten.

Beispiel:

```
aws s3api get-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg C:\Users
\user\Pictures\sailbot.jpg
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

```
C:\>aws s3api get-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg C:\Users\user\Pictures\sailbot.jpg
{
    "AcceptRanges": "bytes",
    "LastModified": "2021-05-10T05:09:31+00:00",
    "ContentLength": 48224,
    "ETag": "\"694d34example91d92d64f342aa234c3\"",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

Verwalten von Buckets und Objekten

Dies sind die allgemeinen Schritte zum Verwalten Ihres Lightsail-Objektspeicher-Buckets:

1. Weitere Informationen über Buckets und Objekte im Amazon Lightsail-Objektspeicherservice. Weitere Informationen zu Buckets finden Sie unter Objektspeicher in Amazon Lightsail.
2. Erfahren Sie mehr über die Namen, die Sie Ihren Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Namensregeln für Buckets in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherservice, indem Sie einen Bucket erstellen. Weitere Informationen finden Sie unter Buckets erstellen in Amazon Lightsail.
4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren.

Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Lightsail-Objektspeicher und Bucket-Berechtigungen in Amazon Lightsail verstehen.

Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

- Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail
- Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail
- Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
- Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
- Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail
- Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail

5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherservice
   - Zugriffsprotokollierungsformat für Buckets im Amazon Lightsail-Objektspeicher-Service
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicher-Service
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail, um Anforderungen zu identifizieren
6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gewährt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets in Amazon Lightsail.
7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unterGrundlegendes zu Objektschlüsselnamen inAmazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Hochladen einer Datei in einen Bucket in Amazon Lightsail
   - Hochladen von Dateien in Buckets in Amazon Lightsail mit mehrteiligem Upload
   - Anzeigen von Objekten in einem Bucket in Amazon Lightsail
   - Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
   - Objekte von einem Bucket in Amazon Lightsail herunterladen

- Filtern von Objekten in einem Bucket in Amazon Lightsail
- Markieren von Objekten in einem Bucket in Amazon Lightsail
- Löschen von Objekten in einem Bucket in Amazon Lightsail

9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.
10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.
11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.
12. Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen in Amazon Lightsail.
13. Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Tarifs Ihres Buckets in Amazon Lightsail.
14. Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.
    - Tutorial: Verbinden einer WordPress-Instance mit einem Amazon Lightsail-Bucket
    - Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Lightsail-Netzwerkverteilung für die Bereitstellung von Inhalten
15. Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

Bucket-Objekte in Amazon Lightsail filtern

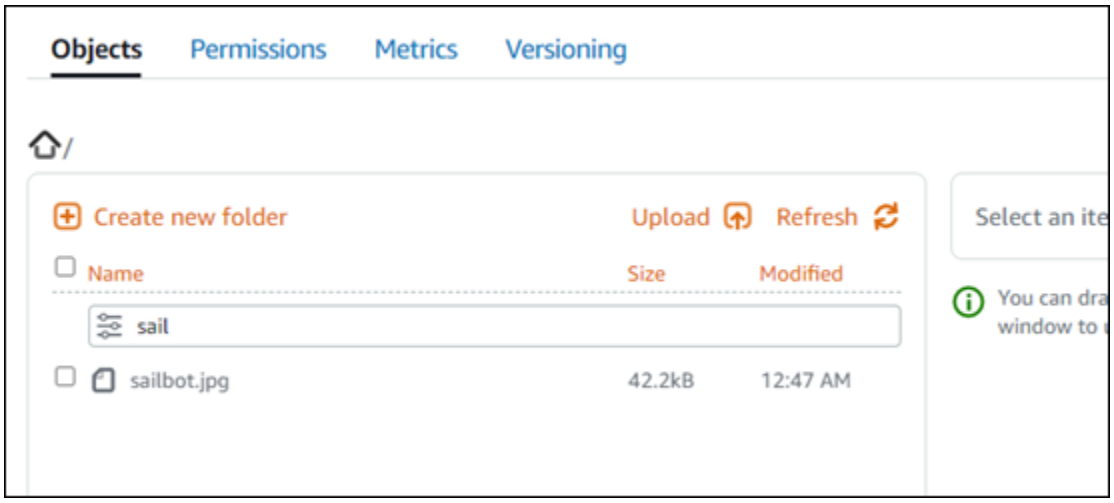
Sie können Filtern verwenden, um Objekte in Ihrem Bucket imAmazon LightsailObjektspeicherdienst zu finden. In dieser Anleitung zeigen wir Ihnen, wie Sie Objekte mittels Lightsail-Konsole und AWS Command Line Interface (AWS CLI) filtern. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Filtern von Objekten mit der Lightsail-Konsole

Vervollständigen Sie das folgende Verfahren, um Objekte in einen Bucket mithilfe derLightsail-Konsole zu filtern.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen des Buckets aus, für den Sie Objekte suchen möchten.
4. In der Registerkarte Objekte, geben Sie ein Objektpräfix in das Textfeld Nach Name filtern ein.

   Die Liste der Objekte in dem Ordner, den Sie gerade anzeigen, wird gefiltert, um dem eingegebenen Text zu entsprechen. Das folgende Beispiel zeigt, dass, wenn Sie`sail` eingeben, wird die Liste der Objekte auf der Seite so gefiltert, dass nur diejenigen angezeigt werden, die mit `sail` starten.



   Um die Liste der Objekte in einem anderen Ordner zu filtern, navigieren Sie zu diesem Ordner. Geben Sie dann das Objektpräfix in das TextfeldNach Name filtern ein.

Filtern von Objekten mit der AWS CLI

Vervollständigen Sie das folgende Verfahren, um Objekte in einen Bucket mithilfe der AWS Command Line Interface (AWS CLI) zu filtern. Führen Sie dazu den Befehl `list-objects-v2` aus. Weitere Informationen finden Sie unter list-objects-v2 in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS Command Line Interface für die Arbeit mit Amazon Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um Objekte aufzulisten, die mit einem bestimmten Objektschlüsselnamen-Präfix beginnen.

```
aws s3api list-objects-v2 --bucket BucketName --prefix ObjectKeyNamePrefix --query
 "Contents[].{Key: Key, Size: Size}"
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *BucketName* – Der Name des Buckets, für das Sie alle Objekte aufführen möchten.
- *ObjectKeyNamePrefix* – Ein Objektschlüsselnamenpräfix, um die Antwort auf Schlüssel zu beschränken, die mit dem angegebenen Präfix beginnen.

> **Note**
>
> Dieser Befehl verwendet die `--query`-Parameter, um die Antwort der `list-objects-v2`-Anforderung auf den Schlüsselwert und die Größe jedes Objekts zu filtern.

Beispiel:

```
aws s3api list-objects-v2 --bucket DOC-EXAMPLE-BUCKET --prefix archived/ --query
 "Contents[].{Key: Key, Size: Size}"
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

```
C:\>aws s3api list-objects-v2  --bucket DOC-EXAMPLE-BUCKET --prefix archived/ --query "Contents[].{Key: Key, Size: Size}"
[
    {
        "Key": "archived/",
        "Size": 0
    },
    {
        "Key": "archived/1_CMoFsPfso.jpg",
        "Size": 2561865
    },
    {
        "Key": "archived/3y1zF4hIPCg.jpg",
        "Size": 6404907
    },
    {
        "Key": "archived/5IHz5WhosQE.jpg",
        "Size": 2377975
    },
    {
        "Key": "archived/sailbot.jpg",
        "Size": 43246
    }
]
```

Verwalten von Buckets und Objekten

Dies sind die allgemeinen Schritte zum Verwalten Ihres Lightsail-Objektspeicher-Buckets:

1. Weitere Informationen über Buckets und Objekte im Amazon Lightsail-Objektspeicherservice. Weitere Informationen zu Buckets finden Sie unter Objektspeicher in Amazon Lightsail.
2. Erfahren Sie mehr über die Namen, die Sie Ihren Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Namensregeln für Buckets in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherservice, indem Sie einen Bucket erstellen. Weitere Informationen finden Sie unter Buckets erstellen in Amazon Lightsail.
4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Lightsail-Objektspeicher und Bucket-Berechtigungen in Amazon Lightsail verstehen.

   Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

   - Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail
   - Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail

- Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
- Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
- Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail
- Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail

5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherservice
   - Zugriffsprotokollierungsformat für Buckets im Amazon Lightsail-Objektspeicher-Service
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicher-Service
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail, um Anforderungen zu identifizieren
6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gewährt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets in Amazon Lightsail.
7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unterGrundlegendes zu Objektschlüsselnamen inAmazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Hochladen einer Datei in einen Bucket in Amazon Lightsail
   - Hochladen von Dateien in Buckets in Amazon Lightsail mit mehrteiligem Upload
   - Anzeigen von Objekten in einem Bucket in Amazon Lightsail
   - Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
   - Objekte von einem Bucket in Amazon Lightsail herunterladen
   - Filtern von Objekten in einem Bucket in Amazon Lightsail
   - Markieren von Objekten in einem Bucket in Amazon Lightsail
   - Löschen von Objekten in einem Bucket in Amazon Lightsail
9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.

10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.
11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.
12. Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen in Amazon Lightsail.
13. Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Tarifs Ihres Buckets in Amazon Lightsail.
14. Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.
    - Tutorial: Verbinden einer WordPress-Instance mit einem Amazon Lightsail-Bucket
    - Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Lightsail-Netzwerkverteilung für die Bereitstellung von Inhalten
15. Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

Objekt-Versionsverwaltung in Amazon Lightsail aktivieren und aussetzen

Die Versioning imAmazon Lightsail-Objektspeicherdienst ermöglicht Ihnen, mehrere Versionen eines Objekts im selben Bucket aufzubewahren. Sie können die Versioning-Feature verwenden, um sämtliche Versionen aller Objekte in Ihren Buckets zu speichern, abzurufen oder wiederherzustellen. Daten lassen sich dank Versioning nach unbeabsichtigten Benutzeraktionen und Anwendungsfehlern leichter wiederherstellen. Wenn Sie das Versioning für einen Bucket aktivieren und der Lightsail-Objektspeicherdienst mehrere Schreibanforderungen für dasselbe Objekt gleichzeitig empfängt, werden alle Objekte gespeichert. Das Versioning ist standardmäßig für Buckets im Lightsail-Objektspeicherdienst deaktiviert, Sie müssen ihn daher explizit aktivieren. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

> **Important**
>
> Wenn Sie die Versioning für einen Bucket aktivieren oder anhalten, der dieEinzelne Objekte können öffentlich gemacht werden (schreibgeschützt)-Zugriffsberechtigung hat,

wird die Berechtigung aufAlle Objekte sind privat zurückgesetzt. Wenn Sie weiterhin die Option haben möchten, einzelne Objekte öffentlich zu machen, müssen Sie die Bucket-Zugriffsberechtigung manuell wieder inEinzelne Objekte können öffentlich gemacht werden (schreibgeschützt) ändern. Weitere Informationen finden Sie unter Konfigurieren von Bucket-Zugriffsberechtigungen.

Deaktivierte, aktivierte und angehaltene Versionen

Bucket-Versioning kann in einem von drei Zuständen in der Lightsail-Konsole sein:

- Deaktiviert (`NeverEnabled` in der API und SDKs)
- Aktiviert (`Enabled` in der API und SDKs)
- Angehalten (`Suspended` in der API und SDKs)

Nachdem Sie das Versioning in einem Bucket aktiviert haben, kann es nicht in einen deaktivierten Zustand zurückkehren. Sie können das Versioning jedoch anhalten. Sie aktivieren und unterbrechen das Versioning auf Bucket-Ebene.

Der Versioning-Status gilt für alle (niemals für eine Untermenge) der Objekte in diesem Bucket. Wenn Sie die Versioning in einem Bucket aktivieren, werden alle neuen Objekte versioniert und mit einer eindeutigen Versions-ID versehen. Objekte, die bereits im Bucket vorhanden sind, wenn das Versioning aktiviert ist, werden immer in Zukunft versioniert. Sie erhalten eine eindeutige Version-ID, wenn sie durch zukünftige Anforderungen geändert werden.

Versions-ID

Wenn Sie das Versioning für einen Bucket aktivieren, generiert der Lightsail-Objektspeicherdienst automatisch eine eindeutige Version-ID für das Objekt, das gespeichert wird. Beispielsweise könnten Sie in einem Bucket zwei Objekte mit demselben Schlüssel haben, aber mit unterschiedlichen Versions-IDs, wie beispielsweise `photo.gif` (Version 111111) und `photo.gif` (Version 121212).

Version-IDs können nicht bearbeitet werden. Diese sind Unicode-, UTF-8-codierte, URL-fähige, nicht einsichtige Zeichenfolgen, die nicht mehr als 1 024 Byte lang sind. Nachfolgend finden Sie ein Beispiel einer Version-ID:

```
3sL4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY+MTRCxf3vjVBH40Nr8X8gdRQBpUMLUo
```

Aktivieren oder anhalten der Objektversioning mithilfe der Lightsail-Konsole

Führen Sie das folgende Verfahren aus, um Objektversioning mithilfe derLightsail-Konsole zu aktivieren oder anzuhalten.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen des Buckets aus, für den Sie das Versioning aktivieren oder anhalten möchten.
4. Wählen Sie die Registerkarte Versioning aus.
5. Führen Sie abhängig vom aktuellen Versioningsstatus Ihres Buckets eine der folgenden Aktionen aus:

   - Wenn das Versioning derzeit angehalten ist oder nicht aktiviert wurde, wählen Sie den Schalter unter dem Abschnitt Objektversioning der Seite, um das Versioning zu aktivieren.
   - Wenn das Versioning derzeit aktiviert ist, wählen Sie den Schalter unter dem Abschnitt Objektversioning der Seite, um das Versioning anzuhalten.

Aktivieren oder anhalten der Objektversioning mithilfe der AWS CLI

Führen Sie das folgende Verfahren aus, um Objekt-Versionsverwaltung mithilfe der AWS Command Line Interface (AWS CLI) zu aktivieren oder anzuhalten. Führen Sie dazu den Befehl `update-bucket` aus. Weitere Informationen finden Sie unter update-bucket in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um Objektversioning zu aktivieren oder anzuhalten.

```
aws lightsail update-bucket --bucket-name BucketName --versioning VersioningState
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *Bucket-Name* - Der Namen des Buckets, für den Sie Objektversioning aktivieren möchten.
- *VersioningState*: Einer der folgenden Punkte:
  - `Enabled`- Aktiviert Objektversioning.
  - `Suspended`- Hält die Objektversioning an, wenn sie zuvor aktiviert wurde.

Beispiel:

```
aws lightsail update-bucket --bucket-name DOC-EXAMPLE-BUCKET --versioning Enabled
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

```
C:\>aws lightsail update-bucket --bucket-name DOC-EXAMPLE-BUCKET --versioning Enabled
{
    "bucket": {
        "resourceType": "Bucket",
        "accessRules": {
            "getObject": "private",
            "allowPublicOverrides": false
        },
        "arn": "arn:aws:lightsail:us-west-2:1example7491:Bucket/f067383e-ee41-4485-b934-example2e2fd",
        "bundleId": "small_1_0",
        "createdAt": "2021-06-29T08:12:39.163000-07:00",
        "url": "https://DOC-EXAMPLE-BUCKET.s3.us-west-2.amazonaws.com",
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "name": "DOC-EXAMPLE-BUCKET",
        "supportCode": "621291663362/DOC-EXAMPLE-BUCKET/small_1_0",
        "tags": [],
        "objectVersioning": "Enabled",
        "ableToUpdateBundle": true
    },
    "operations": [
        {
            "id": "0d53d290-f4b2-43f0-89d2-example43448",
            "resourceName": "DOC-EXAMPLE-BUCKET",
            "resourceType": "Bucket",
            "createdAt": "2021-06-29T08:29:56.241000-07:00",
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "6example3362/DOC-EXAMPLE-BUCKET/small_1_0",
            "operationType": "UpdateBucket",
            "status": "Succeeded",
            "statusChangedAt": "2021-06-29T08:29:56.241000-07:00",
            "errorCode": "",
            "errorDetails": ""
        }
    ]
}
```

Verwalten von Buckets und Objekten

Dies sind die allgemeinen Schritte zum Verwalten Ihres Lightsail-Objektspeicher-Buckets:

1. Weitere Informationen über Buckets und Objekte im Amazon Lightsail-Objektspeicherservice. Weitere Informationen zu Buckets finden Sie unter Objektspeicher in Amazon Lightsail.
2. Erfahren Sie mehr über die Namen, die Sie Ihren Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Namensregeln für Buckets in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherservice, indem Sie einen Bucket erstellen. Weitere Informationen finden Sie unter Buckets erstellen in Amazon Lightsail.

4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Lightsail-Objektspeicher und Bucket-Berechtigungen in Amazon Lightsail verstehen.

   Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

   - Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail
   - Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail
   - Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
   - Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
   - Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail
   - Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail
5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.

   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherservice
   - Zugriffsprotokollierungsformat für Buckets im Amazon Lightsail-Objektspeicher-Service
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicher-Service
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail, um Anforderungen zu identifizieren
6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gewährt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets in Amazon Lightsail.
7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unterGrundlegendes zu Objektschlüsselnamen inAmazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.

   - Hochladen einer Datei in einen Bucket in Amazon Lightsail

- Hochladen von Dateien in Buckets in Amazon Lightsail mit mehrteiligem Upload
- Anzeigen von Objekten in einem Bucket in Amazon Lightsail
- Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
- Objekte von einem Bucket in Amazon Lightsail herunterladen
- Filtern von Objekten in einem Bucket in Amazon Lightsail
- Markieren von Objekten in einem Bucket in Amazon Lightsail
- Löschen von Objekten in einem Bucket in Amazon Lightsail

9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.
10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.
11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.
12. Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen in Amazon Lightsail.
13. Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Tarifs Ihres Buckets in Amazon Lightsail.
14. Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.
    - Tutorial: Verbinden einer WordPress-Instance mit einem Amazon Lightsail-Bucket
    - Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Lightsail-Netzwerkverteilung für die Bereitstellung von Inhalten
15. Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

Wiederherstellen früherer Versionen von Bucket-Objekten in Amazon Lightsail

Wenn Ihr Bucket im Amazon Lightsail-Objektspeicherdienst versionsaktiviert ist, können Sie frühere Versionen eines Objekts wiederherstellen. So stellen Sie eine frühere Version eines Objekts aus unbeabsichtigten Benutzeraktionen oder Anwendungsausfällen wieder her.

Sie können eine frühere Version eines Objekts mithilfe der Lightsail-Konsole. Sie können auch die AWS Command Line Interface (AWS CLI) verwenden und AWS-SDKs stellen eine frühere Version eines Objekts wieder her. Kopieren Sie dazu eine spezifische Version des Objekts in denselben Bucket, und verwenden Sie denselben Objektschlüsselnamen. Dadurch wird die aktuelle Version durch die vorherige Version ersetzt, wodurch die vorherige Version zur aktuellen Version wird. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionsverwaltung in einem Bucket. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Wiederherstellen einer früheren Version eines Objekts mithilfe der Lightsail-Konsole

Vervollständigen Sie das folgende Verfahren, um ein Objekt einschließlich der gespeicherten vorherigen Versionen mithilfe der Lightsail-Konsole zu löschen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen des Buckets aus, für den Sie eine frühere Version eines Objekts wiederherstellen möchten.
4. Verwenden des Fensters Browser Objekte in der Registerkarte Objekte, um zu dem Speicherort des Objekts zu navigieren, das Sie löschen möchten.
5. Fügen Sie ein Häkchen neben dem Objekt hinzu, für das Sie gespeicherten früheren Versionen löschen möchten.
6. Wählen Sie Verwalten im Abschnitt „Versionen“ des Bereichs Informationen zum Objekt.
7. Wählen Sie Restore (Wiederherstellen) aus.
8. Im Fenster Verwalten gespeicherter Objektversionen, das angezeigt wird, fügen Sie ein Häkchen neben den Versionen des Objekts hinzu, das Sie löschen möchten.
9. Klicken Sie auf Weiter.
10. Wählen Sie in der angezeigten Bestätigungsaufforderung Ja, wiederherstellen, um die Objektversion wiederherzustellen. Andernfalls wählen Sie Nein, abbrechen.

Wiederherstellen einer früheren Version eines Objekts mithilfe der AWS CLI

Vervollständigen Sie das folgende Verfahren, um ein Objekt einschließlich der gespeicherten vorherigen Versionen mithilfe der AWS Command Line Interface (AWS CLI) zu löschen. Führen Sie dazu den Befehl `copy-object` aus. Sie müssen die frühere Version des Objekts mithilfe desselben Objektschlüssels in denselben Bucket kopieren. Weitere Informationen finden Sie unter copy-object in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS Command Line Interface für die Arbeit mit Amazon Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um eine frühere Version eines Objekts wiederherzustellen.

```
aws s3api copy-object --copy-source "BucketName/ObjectKey?versionId=VersionId" --
key ObjectKey --bucket BucketName
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *`Bucket-Name`* – Der Namen des Buckets, für den Sie Objektversioning aktivieren möchten. Sie müssen denselben Bucket-Namen für den `--copy-source`- und `--bucket`-Parameter.
- *`ObjectKey`* – Der Name des Objekts, das wiederhergestellt werden soll. Sie müssen denselben Objekt-Schlüssel für den `--copy-source`- und `--key`-Parameter angeben.
- *`VersionId`* – Die ID der vorherigen Objektversion, die Sie auf die aktuelle Version wiederherstellen möchten. Verwenden der`list-object-versions`-Befehl aus, um eine Liste von Versionskennungen für Objekte in Ihrem Bucket zu erhalten.

Beispiel:

```
aws s3api copy-object --copy-source "DOC-EXAMPLE-BUCKET/sailbot.jpg?
versionId=GQWEexample87Mdl8Q_DKdVTiVMi_VyU" -key sailbot.jpg --bucket DOC-EXAMPLE-
BUCKET
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

```
C:\>aws s3api copy-object --copy-source "DOC-EXAMPLE-BUCKET/sailbot.jpg?versionId=GQWEexample87Mdl8Q_DKdVTiVMi_VyU"
--key sailbot.jpg --bucket DOC-EXAMPLE-BUCKET
{
    "CopySourceVersionId": "GQWEcouyrfexampleQ_DKdVTiVMi_VyU",
    "VersionId": "hjL8anKzI1xcXYyexampleDvvqMXSLoi",
    "ServerSideEncryption": "AES256",
    "CopyObjectResult": {
        "ETag": "\"dc5afd388fb3example20cda3fe41c54\"",
        "LastModified": "2021-05-16T06:45:35+00:00"
    }
}
```

Verwalten von Buckets und Objekten

Dies sind die allgemeinen Schritte zum Verwalten Ihres Lightsail-Objektspeicher-Buckets:

1. Weitere Informationen über Buckets und Objekte im Amazon Lightsail-Objektspeicherservice. Weitere Informationen zu Buckets finden Sie unter Objektspeicher in Amazon Lightsail.
2. Erfahren Sie mehr über die Namen, die Sie Ihren Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Namensregeln für Buckets in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherservice, indem Sie einen Bucket erstellen. Weitere Informationen finden Sie unter Buckets erstellen in Amazon Lightsail.
4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Lightsail-Objektspeicher und Bucket-Berechtigungen in Amazon Lightsail verstehen.

   Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

   - Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail
   - Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail
   - Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
   - Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
   - Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail

- Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail

5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherservice
   - Zugriffsprotokollierungsformat für Buckets im Amazon Lightsail-Objektspeicher-Service
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicher-Service
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail, um Anforderungen zu identifizieren
6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gewährt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets in Amazon Lightsail.
7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unterGrundlegendes zu Objektschlüsselnamen inAmazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Hochladen einer Datei in einen Bucket in Amazon Lightsail
   - Hochladen von Dateien in Buckets in Amazon Lightsail mit mehrteiligem Upload
   - Anzeigen von Objekten in einem Bucket in Amazon Lightsail
   - Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
   - Objekte von einem Bucket in Amazon Lightsail herunterladen
   - Filtern von Objekten in einem Bucket in Amazon Lightsail
   - Markieren von Objekten in einem Bucket in Amazon Lightsail
   - Löschen von Objekten in einem Bucket in Amazon Lightsail
9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.
10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.

11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.
12. Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen in Amazon Lightsail.
13. Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Tarifs Ihres Buckets in Amazon Lightsail.
14. Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.
    - Tutorial: Verbinden einer WordPress-Instance mit einem Amazon Lightsail-Bucket
    - Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Lightsail-Netzwerkverteilung für die Bereitstellung von Inhalten
15. Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

Bucket-Objekte in Amazon Lightsail taggen

Markieren Sie Obekte in Ihrem Bucket, um Ihre Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Markieren Sie Objekte, beim Hochladen oder nach dem Hochladen. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Hinzufügen und Löschen von Tags für Objekte mithilfe der Lightsail-Konsole

Vervollständigen Sie das folgende Verfahren, um Objekte in einen Bucket mithilfe der Lightsail-Konsole zu filtern.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen des Buckets aus, für den Sie Objekte markieren möchten.
4. Verwenden des Fensters Browser Objekte in der Registerkarte Objekte, um zu dem Speicherort des Objekts zu navigieren, das Sie löschen möchten.
5. Setzen Sie ein Häkchen neben das Objekt, für das Sie einen Tag hinzufügen oder löschen möchten.

6. Wählen Sie im Bereich Objektinformationen eine der folgenden Optionen unter dem Abschnitt Objekt-Tags:

   - Einfügen oder Bearbeiten (wenn bereits Tags hinzugefügt wurden). Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Speichern um das Tag hinzuzufügen. Wählen Sie andernfalls Abbrechen.
   - Bearbeiten und dann wählen Sie X neben dem Schlüssel-Wert-Tag, das Sie löschen möchten. Wählen Sie Speichern, wenn Sie das Tag gelöscht haben oder wählen Sie Abbrechen, um es nicht zu löschen.

Hinzufügen und Löschen von Tags für Objekte mithilfe der AWS CLI

Vervollständigen Sie das folgende Verfahren, um Objekte von Ihrem Bucket mithilfe der AWS Command Line Interface (AWS CLI) herunterzuladen. Führen Sie dazu die Befehle `put-object-tagging` und `delete-object-tagging` aus. Weitere Informationen finden Sie unter put-object-tagging und delete-object-tagging in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie einen der folgenden Befehle ein:

   - Hinzufügen von Markern zu einem Objekt:

     ```
     aws s3api put-object-tagging --bucket BucketName --key ObjectKey --tagging
      "{\"TagSet\":[{ \"Key\": \"KeyTag\", \"Value\": \"ValueTag\" }]}"
     ```

     Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

     - *Bucket-Name* – Der Name des Buckets, der das Objekt enthält, das Sie mit Tags versehen möchten.

- *Objektschlüssel* – Der vollständige Objektschlüssel des Objekts, das Sie löschen möchten.
- *KeyTag* – Der Schlüsselwert Ihres Tags.
- *ValueTag* – Der Wert Ihres Tags.

- Hinzufügen eines Tags zu einem Objekt:

```
aws s3api put-object-tagging --bucket BucketName --key ObjectKey --tagging
 "{\"TagSet\":[{ \"Key\": \"KeyTag1\", \"Value\": \"ValueTag1\" }, { \"Key\":
 \"KeyTag2\", \"Value\": \"ValueTag2\" }]}"
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *Bucket-Name* – Der Name des Buckets, der das Objekt enthält, das Sie mit Tags versehen möchten.
- *Objektschlüssel* – Der vollständige Objektschlüssel des Objekts, das Sie löschen möchten.
- *KeyTag1* – Der Schlüsselwert Ihres ersten Tags.
- *ValueTag1* – Der Wert Ihres ersten Tags.
- *KeyTag2* – Der Schlüsselwert Ihres zweiten Tags.
- *ValueTag2* – Der Wert Ihres ersten zweiten Tags.

- Löschen von Tags von einem Objekt:

```
aws s3api delete-object-tagging --bucket BucketName --key ObjectKey
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *Bucket-Name* – Der Name des Buckets, der das Objekt enthält, das Sie mit Tags versehen möchten.
- *Objektschlüssel* – Der vollständige Objektschlüssel des Objekts, das Sie löschen möchten.

Beispiel:

```
aws s3api delete-object --bucket DOC-EXAMPLE-BUCKET --key nptLmg6jqDo.jpg --tagging
 "{\"TagSet\":[{ \"Key\": \"Importance\", \"Value\": \"High\" }]}"
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

```
C:\>aws s3api put-object-tagging --bucket DOC-EXAMPLE-BUCKET  --key nptLmg6jqDo.jpg
--tagging "{\"TagSet\":[{ \"Key\": \"Importance\", \"Value\": \"High\" }]}"
{
    "VersionId": "9nL2d41NuZdhdk4HS3kZIwOxJeS1kCkm"
}
```

Verwalten von Buckets und Objekten

Dies sind die allgemeinen Schritte zum Verwalten Ihres Lightsail-Objektspeicher-Buckets:

1. Weitere Informationen über Buckets und Objekte im Amazon Lightsail-Objektspeicherservice. Weitere Informationen zu Buckets finden Sie unter Objektspeicher in Amazon Lightsail.
2. Erfahren Sie mehr über die Namen, die Sie Ihren Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Namensregeln für Buckets in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherservice, indem Sie einen Bucket erstellen. Weitere Informationen finden Sie unter Buckets erstellen in Amazon Lightsail.
4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Lightsail-Objektspeicher und Bucket-Berechtigungen in Amazon Lightsail verstehen.

   Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

   - Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail
   - Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail
   - Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
   - Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
   - Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail
   - Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail

5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherservice
   - Zugriffsprotokollierungsformat für Buckets im Amazon Lightsail-Objektspeicher-Service
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicher-Service
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail, um Anforderungen zu identifizieren
6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gewährt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets in Amazon Lightsail.
7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unterGrundlegendes zu Objektschlüsselnamen inAmazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Hochladen einer Datei in einen Bucket in Amazon Lightsail
   - Hochladen von Dateien in Buckets in Amazon Lightsail mit mehrteiligem Upload
   - Anzeigen von Objekten in einem Bucket in Amazon Lightsail
   - Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
   - Objekte von einem Bucket in Amazon Lightsail herunterladen
   - Filtern von Objekten in einem Bucket in Amazon Lightsail
   - Markieren von Objekten in einem Bucket in Amazon Lightsail
   - Löschen von Objekten in einem Bucket in Amazon Lightsail
9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.
10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.
11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.

12. Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen in Amazon Lightsail.
13. Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Tarifs Ihres Buckets in Amazon Lightsail.
14. Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.
    - Tutorial: Verbinden einer WordPress-Instance mit einem Amazon Lightsail-Bucket
    - Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Lightsail-Netzwerkverteilung für die Bereitstellung von Inhalten
15. Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

Konfigurieren des Ressourcenzugriffs für ein Lightsail-Bucket

Fügen Sie einen Amazon Lightsail-Instance auf eineLightsail-Bucket an, um ihm vollen programmatischen Zugriff auf den Bucket und seine Objekte zu geben. Wenn Sie Instances an Buckets anfügen, müssen Sie keine Anmeldeinformationen wie Zugriffsschlüssel verwalten. Die Instances und der Bucket müssen sich in der gleichen AWS-Region befinden. Sie können keine Instances an Buckets anfügen, die sich in einer anderen Region befinden.

Resource access (Ressourcenzugriff) ist ideal, wenn Sie Software oder ein Plug-In auf Ihrer Instance konfigurieren, um Dateien direkt in Ihren Bucket hochzuladen. Wollen Sie beispielsweise eine WordPress-Instance so konfigurieren, dass Mediendateien in einem Bucket gespeichert werden. Weitere Informationen finden Sie im Tutorial: Verbinden Sie einen Bucket mit Ihrer WordPress-Instance.

Weitere Informationen zu Berechtigungsoptionen finden Sie unter Bucket-Berechtigungen. Weitere Informationen zu bewährten Methoden für die Sicherheit finden Sie unter Bewährte Methoden für die Sicherheit für Objektspeicher. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Konfigurieren des Resource access (Ressourcenzugriff) für einen Bucket

Führen Sie das folgende Verfahren durch, um Zugriffsschlüssel für einen Bucket zu erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.

2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen des Buckets aus, für den Sie den Resource access (Ressourcenzugriff) konfigurieren möchten.
4. Wählen Sie die Registerkarte Permissions (Berechtigungen).

   Der Abschnitt Resource access (Ressourcenzugriff) der Seite zeigt die Instances an, die – falls vorhanden – derzeit mit dem Bucket verknüpft sind.
5. Klicken Sie auf Hinzufügen von Instance, um eine Instance an den Bucket anzufügen.
6. Im Dropdown-Menü Wählen Sie eine Instance aus, wählen Sie die Instance aus, die Sie an den Bucket anfügen möchten.

   > **Note**
   >
   > Sie können Instances zuordnen, die sich nur im ausgeführten oder angehaltenen Zustand befinden. Darüber hinaus können Sie nur Instances zuordnen, die sich in derselben AWS-Region wie der Bucket befinden.
7. Wählen Sie Attach (Anfügen) zum Anfügen des Datenträgers an die ausgewählte Instance. Wählen Sie andernfalls Abbrechen.

   Die Instance hat nach dem Anhängen vollen Zugriff auf den Bucket und seine Objekte. Sie können Software oder ein Plug-In auf Ihrer Instance konfigurieren, um Dateien in Ihrem Bucket programmgesteuert hochzuladen und darauf zuzugreifen. Wollen Sie beispielsweise eine WordPress-Instance so konfigurieren, dass Mediendateien in einem Bucket gespeichert werden. Weitere Informationen finden Sie im Tutorial: Verbinden Sie einen Bucket mit Ihrer WordPress-Instance.

Ändern des Plans Ihres Lightsail-Buckets

Im Amazon Lightsail-Objektspeicherdienst gibt der Speicherplan eines Buckets die monatlichen Kosten, das Speicherplatzkontingent und das Datenübertragungskontingent an. Sie können den Bucket-Plan innerhalb Ihres monatlichen AWS-Abrechnungszeitraums nur einmal ändern. Wenn Sie den Speicherplan Ihres Buckets ändern, werden die Speicherplatz- und Netzwerkübertragungskontingente zurückgesetzt. Die Kosten für überschüssige Speicherplatz und Datenübertragungen, die Sie möglicherweise durch die Verwendung des vorherigen Speicherplans anfallen, werden jedoch nicht gedeckt.

Ändern Sie den Plan Ihres Buckets, wenn dieser konsistent über seinen Speicherplatz oder das Datenübertragungskontingent geht oder wenn die Nutzung Ihres Buckets konsistent im unteren Bereich des Speicherplatzes oder der Datenübertragungskontingents liegt. Da in Ihrem Bucket möglicherweise unvorhersehbare Nutzungsschwankungen auftreten, wird dringend empfohlen, den Speicherplan Ihres Buckets nur als langfristige Strategie zu aktualisieren, anstatt als kurzfristige, monatliche Kostensenkungsmaßnahme. Wählen Sie einen Speicherplan, der Ihrem Bucket ausreichend Speicherplatz und Datenübertragungskontingent für eine lange Zeit zur Verfügung stellt.

Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Ändern des Speicherplans Ihres Buckets mithilfe der Lightsail-Konsole

Vervollständigen Sie den folgenden Vorgang, um den Bucket mit derLightsail-Konsole zu löschen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen der Datenbank aus, für die Sie die Pläne ändern möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Seite der Instance-Verwaltung aus.
5. Wählen Sie Ändern des Speicherplans.
6. Wählen Sie in der angezeigten Bestätigungsaufforderung Ja, ändern, um Ihren Bucket-Speicherplan weiter zu ändern. Andernfalls wählen Sie Nein, abbrechen.
7. Wählen Sie den Stack aus, den Sie aktualisieren möchten, wählen Sie anschließend Plan auswählen.
8. Wählen Sie in der angezeigten Bestätigungsaufforderung Ja, anwenden, um die Änderung auf Ihren Bucket anzuwenden oder Nein, zurück, um sie nicht anzuwenden.

Ändern Sie den Speicherplan Ihres Buckets mithilfe derAWS CLI

Vervollständigen Sie das folgende Verfahren, um Ihren Bucket mithilfe der AWS Command Line Interface (AWS CLI) zu löschen. Führen Sie dazu den Befehl `update-bucket-bundle` aus. Beachten Sie, dass einen Bucket-Speicherplan in der API als Bucket-Bündel bezeichnet wird. Weitere Informationen finden Sie unter update-bucket-bundle in der AWS CLI -Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um den Plan Ihres Buckets zu ändern.

```
aws lightsail update-bucket-bundle --bucket-name BucketName --bundle-id BundleID
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *Bucket-Name* – Name des Buckets, für den Sie den Speicherplan aktualisieren möchten.
- *Bündel-ID* – Die ID des neuen Bucket-Pakets, das Sie auf den Bucket anwenden möchten. Verwenden Sie den `get-bucket-bundles`-Befehl, um eine Liste verfügbarer Bucket-Bündel und deren IDs anzuzeigen. Weitere Informationen finden Sie unter create-bucket in der AWS CLI-Befehlsreferenz.

Beispiel:

```
aws lightsail update-bucket-bundle --bucket-name DOC-EXAMPLE-BUCKET --bundle-
id medium_1_0
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

```
C:\>aws lightsail update-bucket-bundle --bucket-name DOC-EXAMPLE-BUCKET --bundle-id medium_1_0

{
    "operations": [
        {
            "id": "8example-8176-48bd-b1da-exampleb8404",
            "resourceName": "DOC-EXAMPLE-BUCKET",
            "resourceType": "Bucket",
            "createdAt": "2021-06-30T12:05:57.362000-07:00",
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "62example362/DOC-EXAMPLE-BUCKET/medium_1_0",
            "operationType": "UpdateBucketBundle",
            "status": "Succeeded",
            "statusChangedAt": "2021-06-30T12:05:57.362000-07:00",
            "errorCode": "",
            "errorDetails": ""
        }
    ]
}
```

Zugriffsberechtigungen für Lightsail-Buckets konfigurieren

Verwenden Sie Bucket-Zugriffsberechtigungen, um den öffentlichen (nicht authentifizierten) schreibgeschützten Zugriff auf Objekte in einem Bucket zu steuern. Sie können einen Bucket privat oder öffentlich machen (schreibgeschützt). Sie können einen Bucket auch privat machen, während Sie die Möglichkeit haben, einzelne Objekte öffentlich zu machen (schreibgeschützt).

> **Important**
>
> Wenn Sie einen Bucket öffentlich machen (schreibgeschützt), machen Sie alle Objekte im Bucket für jeden Benutzer im Internet über die URL des Buckets lesbar (z. B. `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`) enthalten. Machen Sie einen Bucket nicht öffentlich (schreibgeschützt), wenn Sie nicht möchten, dass jemand im Internet Zugriff auf Ihre Objekte hat.

Weitere Informationen zu Berechtigungsoptionen finden Sie unter Bucket-Berechtigungen. Weitere Informationen zu bewährten Methoden für die Sicherheit finden Sie unter Bewährte Methoden für die Sicherheit für Objektspeicher. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

> **Important**
>
> Lightsail-Objektspeicherressourcen berücksichtigen sowohl Lightsail-Bucket-Zugriffsberechtigungen als auch Amazon-S3-Konfigurationen zum Blockieren des öffentlichen Zugriffs auf Kontoebene, wenn Sie den öffentlichen Zugriff zulassen oder verweigern. Weitere Informationen finden Sie unter Blockieren des öffentlichen Zugriffs für Buckets.

Zugriffsberechtigungen für Buckets

Führen Sie das folgende Verfahren durch, um Zugriffsschlüssel für einen Bucket zu erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen des Buckets aus, für den Sie Zugriffsberechtigungen konfigurieren möchten.
4. Wählen Sie die Registerkarte Permissions (Berechtigungen).

   Der Abschnitt Zugriffsberechtigungen für Buckets der Seite zeigt die aktuell konfigurierte Zugriffsberechtigung für den Bucket an.
5. Klicken Sie aufBerechtigung ändern, um die Bucket-Zugriffsberechtigungen zu ändern.
6. Wählen Sie eine der folgenden Optionen:

   - All objects are private (Alle Objekte sind privat) — Alle Objekte im Bucket sind nur von Ihnen oder jedem, auf den Sie Zugriff gewähren, lesbar.
   - Einzelne Objekte können öffentlich gemacht werden (schreibgeschützt)— Objekte im Bucket können nur von Ihnen oder jedem Benutzer gelesen werden, auf den Sie Zugriff gewähren, es sei denn, Sie geben ein einzelnes Objekt an, das öffentlich sein soll (schreibgeschützt). Weitere Informationen zu den Zugriffsberechtigungen für einzelne Objekte finden Sie unter Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket.

     Wir empfehlen Ihnen, den Einzelne Objekte können öffentlich gemacht werden (schreibgeschützt) nur, wenn Sie eine bestimmte Notwendigkeit haben, dies zu tun, z. B. nur einige der Objekte in Ihrem Bucket öffentlich zu machen, während alle anderen Objekte privat bleiben. Zum Beispiel erfordern einige WordPress-Plug-Ins, dass Ihr Bucket erlaubt, einzelne Objekte öffentlich zu machen. Weitere Informationen finden Sie unter Tutorial: Verbinden

Ihrer WordPress-Instance mit einem Bucket und Tutorial: Verwenden eines Buckets mit einer Netzwerkverteilung für die Bereitstellung von Inhalten.

- Alle Objekte sind öffentlich (schreibgeschützt)— Alle Objekte im Bucket sind für jedermann im Internet lesbar.

> **Important**
>
> Wenn Sie einen Bucket öffentlich machen (schreibgeschützt), machen Sie alle Objekte im Bucket für jeden Benutzer im Internet über die URL des Buckets lesbar (z. B. `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`) enthalten. Machen Sie einen Bucket nicht öffentlich (schreibgeschützt), wenn Sie nicht möchten, dass jemand im Internet Zugriff auf Ihre Objekte hat.

7. Wählen Sie Speichern, um die Änderung zu speichern. Wählen Sie andernfalls Abbrechen.

Die folgenden Änderungen werden je nachdem, in welche Bucket-Zugriffsberechtigung Sie ändern, implementiert:

- All objects are private (Alle Objekte sind privat) – Alle Objekte im Bucket werden privat, auch wenn sie zuvor mit einer Öffentlich (schreibgeschützt) Zugriffsberechtigung für einzelne Objekte konfiguriert wurden.
- Einzelne Objekte können öffentlich gemacht werden (schreibgeschützt) – Objekte, die zuvor mit einer Öffentlich (schreibgeschützt) Zugriffsberechtigung für einzelne Objekte konfiguriert waren, werden öffentlich. Sie können jetzt Zugriffsberechtigungen für einzelne Objekte konfigurieren.
- Alle Objekte sind privat – Alle Objekte im Bucket werden öffentlich (schreibgeschützt), auch wenn sie zuvor mit einer Privat Zugriffsberechtigung für einzelne Objekte konfiguriert wurden.

Weitere Informationen zu den Zugriffsberechtigungen für einzelne Objekte finden Sie unter Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket.

Konfigurieren von kontoübergreifendem Zugriff für ein Lightsail-Bucket

Verwendung des kontoübergreifenden Zugriffs, um anderen AWS-Konten und deren Benutzern Lesezugriff auf alle Objekte in einem Bereich zu gewähren. Der kontoübergreifende Zugriff ist ideal, wenn Sie Objekte mit einem anderen AWS-Konto teilen möchten. Wenn Sie kontoübergreifenden Zugriff auf ein anderes AWS-Konto gewähren, haben Benutzer in diesem Konto über die URL des Buckets schreibgeschützten Zugriff auf Objekte in einem Bucket (z. B. `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`). Sie können Bucketzugriff auf maximal 10 AWS-Konten gewähren.

Weitere Informationen zu Berechtigungsoptionen finden Sie unter Bucket-Berechtigungen. Weitere Informationen zu bewährten Methoden für die Sicherheit finden Sie unter Bewährte Methoden für die Sicherheit für Objektspeicher. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Konfigurieren von für den kontoübergreifenden Zugriff

Führen Sie das folgende Verfahren durch, um Zugriffsschlüssel für einen Bucket zu erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen des Buckets aus, für den Sie kontoübergreifenden Zugriff konfigurieren möchten.
4. Wählen Sie die Registerkarte Permissions (Berechtigungen).

   Der Abschnitt Kontoübergreifender Zugriff der Seite zeigt die AWS-Konto-IDs an, die, falls vorhanden, derzeit für den Zugriff auf den Bucket konfiguriert sind.
5. Wählen Sie Kontoübergreifenden Zugriff hinzufügen, um den Zugriff auf den Bucket für ein anderes AWS-Konto zu gewähren.
6. Geben Sie im Dialogfeld Konto-ID die ID des AWS-Kontos ein, für das Sie Zugriff gewähren möchten.
7. Klicken Sie auf Save, um Zugriff zu gewähren. Wählen Sie andernfalls Abbrechen.

   Die AWS-Konto-ID, die Sie hinzugefügt haben, wird im Abschnitt Kontoübergreifender Zugriff der Seite aufgelistet. Um den kontoübergreifenden Zugriff für ein AWS-Konto zu entfernen, wählen Sie das Symbol Löschen (Mülleimer) neben der AWS-Konto-ID, die Sie entfernen möchten.

Konfigurieren von Zugriffsberechtigungen für einzelne Bucket-Objekte in Lightsail

Verwenden Sie Zugriffsberechtigungen für einzelne Objekte, um den öffentlichen (nicht authentifizierten) schreibgeschützten Zugriff auf einzelne Objekte in einem Bucket zu steuern. Sie können einzelne Objekte in einem Bucket privat oder öffentlich machen (schreibgeschützt).

> **Important**
>
> Zugriffsberechtigung für einzelne Objekte können nur konfiguriert werden, wenn die Zugriffsberechtigung eines Buckets auf Einzelne Objekte können öffentlich gemacht werden (schreibgeschützt) gesetzt ist. Weitere Informationen zu Bucket-Berechtigungsoptionen finden Sie unter Bucket-Berechtigungen. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Es wird empfohlen, Zugriffsberechtigung für einzelne Objekte nur dann zu konfigurieren, wenn Sie eine bestimmte Notwendigkeit haben, z. B. nur einige der Objekte in Ihrem Bucket öffentlich zu machen, während alle anderen Objekte privat bleiben. Zum Beispiel erfordern einige WordPress-Plug-Ins, dass Ihr Bucket erlaubt, einzelne Objekte öffentlich zu machen. Weitere Informationen finden Sie unter Tutorial: Verbinden Ihrer WordPress-Instance mit einem Bucket und Tutorial: Verwenden eines Buckets mit einer Netzwerkverteilung für die Bereitstellung von Inhalten.

Weitere Informationen zu Berechtigungsoptionen finden Sie unter Bucket-Berechtigungen. Weitere Informationen zu bewährten Methoden für die Sicherheit finden Sie unter Bewährte Methoden für die Sicherheit für Objektspeicher. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Konfigurieren der Zugriffsberechtigung für einzelne Objekte

Führen Sie das folgende Verfahren aus, um Zugriffsberechtigungen für ein einzelnes Objekt in einem Bucket zu konfigurieren. Ein Beispiel für eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gibt, einen Bucket in Lightsail zu verwalten, finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen des Buckets aus, für den Sie Zugriffsberechtigungen für ein einzelnes Objekt konfigurieren möchten.

4. Wählen Sie dieObjekte-Tag.
5. Fügen Sie ein Häkchen neben dem Objekt hinzu, für das Sie eine Zugriffsberechtigung konfigurieren möchten.

   Im Objektinformationsbereich werden die aktuellen Zugriffsberechtigungen für das Objekt angezeigt.
6. Klicken Sie auf Bearbeiten im Berechtigungen des Objektinformationsbereichs, um die Zugriffsberechtigung für das Objekt zu ändern.

   > **Note**
   >
   > Wenn die Bearbeitungsoption nicht verfügbar ist, lässt die Zugriffsberechtigung Ihres Buckets keine Zugriffsberechtigung für einzelne Objekte zu. Um Zugriffsberechtigung für einzelne Objekten zu konfigurieren, muss die Bucket-Zugriffsberechtigung auf Einzelne Objekte können öffentlich gemacht werden (schreibgeschützt) gesetzt werden. Weitere Informationen finden Sie unter Konfigurieren von Bucket-Zugriffsberechtigungen.
7. Wählen Sie im Berechtigung Auswählen das Dropdown-Menü Status und wählen Sie dann eine der folgenden Optionen aus:

   - Privat— Das Objekt ist nur von Ihnen oder jedem, auf den Sie Zugriff gewähren, lesbar.
   - Öffentlich (schreibgeschützt) — Das Objekt ist von jedem auf der Welt lesbar.
8. Wählen Sie Speichern, um die Änderung zu speichern. Wählen Sie andernfalls Abbrechen.

   Die Einstellung Zugriffsberechtigungen für Buckets des Buckets hat folgende Auswirkungen auf Zugriffsberechtigung für einzelne Objekte:

   - Wenn Sie die Bucket-Zugriffsberechtigung zu All objects are private (Alle Objekte sind privat) ändern, werden alle Objekte im Bucket privat, auch wenn sie mit einer Öffentlich (schreibgeschützt) Zugriffsberechtigung für einzelne Objekte konfiguriert wurden. Zugriffsberechtigung für einzelne Objekte, die konfiguriert wurden, werden jedoch beibehalten. Wenn Sie beispielsweise die Bucket-Zugriffsberechtigung zurück in Einzelne Objekte können öffentlich gemacht werden (schreibgeschützt), werden alle Objekte mit einem Öffentlich (schreibgeschützt) individuelle Zugriffsberechtigungen werden wieder öffentlich lesbar.
   - Wenn Sie die Bucket-Zugriffsberechtigung zu Alle Objekte sind öffentlich (schreibgeschützt) ändern, werden alle Objekte im Bucket öffentlich (schreibgeschützt), auch wenn sie mit einer Privat Zugriffsberechtigung für einzelne Objekte konfiguriert wurden.

Weitere Informationen zu den Zugriffsberechtigungen für Objekte finden Sie unter Konfigurieren von Bucket-Zugriffsberechtigungen.

Laden Sie Dateien mit mehrteiligem Upload in einen Lightsail-Bucket hoch

Mit dem mehrteiligen Upload können Sie eine einzelne Datei als Satz aus mehreren Teilen in Ihren Bucket hochladen. Jeder Teil ist ein zusammenhängender Teil der Daten des Objekts. Sie können diese Objektteile unabhängig und in beliebiger Reihenfolge hochladen. Wenn die Übertragung eines Teils fehlschlägt, können Sie das Teil erneut übertragen, ohne dass dies Auswirkungen auf andere Teile hat. Nachdem alle Teile Ihrer Datei hochgeladen sind, baut Amazon S3 diese Teile zusammen und erstellt das Objekt in Ihrem Bucket in Amazon Lightsail. Wenn Ihre Objektgröße 100 MB erreicht, sollten Sie in der Regel mehrteilige Uploads verwenden, anstatt das Objekt in einem einzigen Vorgang hochzuladen. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Die Nutzung mehrteiliger Uploads bietet die folgenden Vorteile:

- Verbesserter Durchsatz - Sie können die Teile parallel hochladen, um den Durchsatz zu erhöhen.
- Schnelle Wiederherstellung bei Netzwerkproblemen - Die kleinere Teilegröße minimiert die Auswirkungen eines Neustarts eines fehlgeschlagenen Uploads aufgrund eines Netzwerkfehlers.
- Hochladen im Laufe der Zeit - Sie können Dateiteile über die Zeit hochladen. Nachdem Sie einen mehrteiligen Upload initiiert haben, haben Sie 24 Stunden Zeit, um den mehrteiligen Upload fertigzustellen.
- Starten Sie einen Upload, bevor Sie die endgültige Objektgröße kennen. Sie können ein Objekt hochladen, während Sie es noch erstellen.

Sie sollten den mehrteiligen Upload wie folgt verwenden:

- Wenn Sie große Objekte über ein stabiles Netzwerk mit hoher Bandbreite hochladen, können Sie einen mehrteiligen Upload verwenden, um die Nutzung der verfügbaren Bandbreite zu maximieren. Hierzu laden Sie Objektteile parallel hoch, um von einer Multi-Threading-Leistung zu profitieren.
- Wenn Sie einen Upload über ein instabiles Netzwerk ausführen, können Sie einen mehrteiligen Upload verwenden, um die Resilienz in Bezug auf Netzwerkfehler durch Vermeidung von Neustarts der Uploads zu vermeiden. Wenn Sie mehrteilige Uploads verwenden, müssen Sie nur die Teile

erneut hochladen, deren Upload unterbrochen wurde. Es besteht keine Notwendigkeit, von vorne zu beginnen oder die gesamte Datei erneut hochzuladen.

Inhalt

Mehrteiliger Upload-Prozess

Der mehrteilige Upload ist ein dreistufiger Prozess, der Amazon-S3-Aktionen verwendet, um Dateien in Ihren Bucket in Lightsail hochzuladen:

1. Starten Sie den mehrteiligen Upload mit derCreateMultipartUploadAktion.
2. Laden Sie die Dateiteile mit der Aktion UploadPart hoch.
3. Schließen Sie den mehrteiligen Upload mit der Aktion CompleteMultipartUpload.

> **Note**
>
> Sie können einen mehrteiligen Upload beenden, nachdem Sie ihn mithilfe der Aktion AbortMultipartUpload initiiert haben.

Wenn die mehrteilige Upload-Anforderung abgeschlossen ist, konstruiert Amazon Simple Storage Service das Objekt aus den hochgeladenen Teilen. Dann können Sie auf das Objekt genauso zugreifen, wie Sie auf jedes andere Objekt in Ihrem Bucket zugreifen würden.

Sie können alle laufenden mehrteiligen Uploads auflisten oder eine Liste der Teile anfordern, die Sie für einen bestimmten Multipart-Upload hochgeladen haben. Alle Vorgänge werden in diesem Abschnitt erklärt.

Initiieren des mehrteiligen Uploads

Wenn Sie eine Anforderung zum Initiieren eines mehrteiligen Uploads senden, gibt Amazon Simple Storage Service eine Antwort mit einer Upload-ID zurück. Dies ist eine eindeutige Kennung für Ihren mehrteiligen Upload. Sie müssen diese Upload-ID immer angeben, wenn Sie Teile hochladen, die Teile auflisten, einen Upload abschließen oder einen Upload abbrechen. Wenn Sie Metadaten bereitstellen möchten, die das hochzuladende Objekt beschreiben, müssen sie in der Anforderung auf Initiierung des mehrteiligen Uploads angegeben werden.

Teile hochladen

Beim Hochladen eines Teils müssen Sie zusätzlich zur Upload-ID eine Teilenummer angeben. Sie können jede Teilenummer zwischen 1 und 10.000 wählen. Die Teilenummer identifiziert eindeutig einen Teil und seine Position im Objekt, das Sie hochladen. Die von Ihnen gewählte Teilenummer muss nicht fortlaufend sein (möglich sind z. B. 1, 5 und 14). Wenn Sie einen neuen Teil mit derselben Teilenummer hochladen wie bereits einmal zuvor, wird der früher hochgeladene Teil überschrieben.

Wenn Sie einen Teil hochladen, gibt Amazon Simple Storage Service einen ETag-Header in der Antwort zurück. Für jeden Teilupload müssen Sie die Teilenummer und den ETag-Wert notieren. Sie müssen diese Werte in die spätere Anforderung einschließen, um den mehrteiligen Upload abzuschließen.

> **Note**
>
> Alle hochgeladenen Teile eines mehrteiligen Uploads werden in Ihrem Bucket gespeichert. Sie belegen den Speicherplatz Ihres Buckets, bis Sie den Upload abgeschlossen haben, den Upload beenden oder die Upload-Zeitüberschreitung überschritten haben. Weitere Informationen finden Sie unter Aufbewahrung eines mehrteiligen Uploads weiter unten in diesem Leitfaden.

Abschließen eines mehrteiligen Uploads

Wenn Sie einen mehrteiligen Upload abschließen, erstellt Amazon Simple Storage Service ein Objekt, indem die Teile in aufsteigender Reihenfolge auf Grundlage der Teilenummer verkettet werden. Wenn Sie Metadaten für das Objekt bei der Initiierung des mehrteiligen Uploads bereitgestellt haben, verknüpft Amazon Simple Storage Service die Metadaten mit dem Objekt. Nach einer erfolgreich ausgeführten Abschlussanforderung sind die Teile nicht mehr vorhanden.

Ihre Anfrage auf Abschluss des mehrteiligen Uploads muss die Upload-ID und eine Liste der Teilenummern mit den entsprechenden ETag-Werten enthalten. Die Antwort von Amazon Simple Storage Service enthält einen ETag, der die kombinierten Objektdaten eindeutig identifiziert. Dieses ETag ist nicht unbedingt ein MD5-Hash der Objektdaten.

Sie können einen mehrteiligen Upload auch abbrechen. Wenn Sie einen mehrteiligen Upload abbrechen, können Sie mit dieser Upload-ID keine Teile mehr hochladen. Der gesamte Speicher für jeden Teil des abgebrochenen mehrteiligen Uploads wird freigegeben. Wenn der mehrteilige Upload abgebrochen wird, während Teile hochgeladen werden, können diese Uploads auch nach dem Abbruch erfolgreich abgeschlossen werden oder fehlschlagen. Um den von allen Teilen verbrauchten Speicherplatz freizugeben, dürfen Sie einen mehrteiligen Upload erst dann abbrechen, wenn alle Uploads abgeschlossen wurden.

Auflistungen mehrteiliger Uploads

Sie können alle Teile eines bestimmten Multipart-Uploads oder alle laufenden mehrteiligen Uploads auflisten. Die Operation für die Teileauflistung gibt die Teileinformationen zurück, die Sie für einen bestimmten mehrteiligen Upload hochgeladen haben. Für jeden Abruf einer Teileauflistung gibt Amazon Simple Storage Service die Teileinformationen für einen angegebenen mehrteiligen Upload bis zu maximal 1 000 Teilen zurück. Wenn im Multipart-Upload mehr als 1.000 Teile vorhanden sind, müssen Sie eine Reihe von Anforderungen auf Teileauflistung senden, um alle Teile abzurufen. Beachten Sie, dass die zurückgegebene Teileauflistung keine Teile enthält, die noch nicht vollständig hochgeladen wurden. Bei Verwendung der Operation Mehrteilige Uploads auflisten können Sie eine Liste aller mehrteiligen Uploads in Bearbeitung erhalten.

Ein mehrteiliger Upload in Verarbeitung ist ein Upload, den Sie gestartet haben, der aber noch nicht abgeschlossen ist oder abgebrochen wurde. Jeder Anforderung gibt bis zu 1.000 mehrteilige Uploads zurück. Wenn mehr als 1 000 mehrteilige Uploads vorhanden sind, müssen Sie zusätzliche Anforderungen senden, um die verbleibenden mehrteiligen Uploads abzurufen. Verwenden Sie die zurückgegebene Liste nur zur Überprüfung. Sie sollten das Ergebnis dieser Auflistung nicht verwenden, wenn Sie eine Anforderung für den Abschluss eines mehrteiligen Uploads senden. Halten Sie sich stattdessen an Ihre eigene Liste der Teilenummern, die Sie beim Hochladen von

Teilen angegeben haben, und die diesbezüglichen ETag-Werte, die Amazon Simple Storage Service zurückgegeben hat.

Gleichzeitige mehrteilige Upload-Vorgänge

In einer verteilten Entwicklungsumgebung ist es für Ihre Anwendung möglich, mehrere Updates gleichzeitig für dasselbe Objekt zu initiieren. Ihre Anwendung kann möglicherweise mehrere Multipart-Uploads mit demselben Objektschlüssel initiieren. Für jeden dieser Uploads kann Ihre Anwendung Teile hochladen und eine Anfrage auf Abschluss des Uploads an Amazon Simple Storage Service senden, um das Objekt zu erstellen. Wenn die Buckets die Versioning aktiviert haben, wird beim Abschluss eines Multipart-Uploads immer eine neue Version erstellt. Bei Buckets, für die kein Versioning aktiviert ist, kann es sein, dass andere Anforderungen vorrangig sind, wie zum Beispiel Anforderungen, die nach Initiierung bis zum Abschluss eines mehrteiligen Uploads empfangen werden.

> **Note**
>
> Es ist möglich, dass andere Anforderungen Vorrang haben, z. B. Anforderungen, die empfangen werden, nachdem Sie einen mehrteiligen Upload initiiert haben und bevor er abgeschlossen ist. Beispielsweise kann ein anderer Vorgang einen Schlüssel löschen, nachdem Sie einen mehrteiligen Upload mit diesem Schlüssel initiiert haben und bevor der mehrteilige Upload abgeschlossen ist. In diesem Fall kann die Antwort für den Abschluss des mehrteiligen Uploads möglicherweise eine erfolgreiche Objekterstellung anzeigen, ohne dass Sie das Objekt je zu Ende bekommen haben.

Aufbewahrung eines mehrteiligen Uploads

Alle hochgeladenen Teile eines mehrteiligen Uploads werden in Ihrem Bucket gespeichert. Sie belegen den Speicherplatz Ihres Buckets, bis Sie den Upload abgeschlossen haben, den Upload beenden oder das Upload-Zeitlimit überschreitet. Bei einem mehrteiligen Upload wird das Timeout überschritten, und der mehrteilige Upload wird nach 24 Stunden nach der Erstellung gelöscht. Wenn Sie einen mehrteiligen Upload beenden oder das Timeout beenden, werden alle hochgeladenen Teile gelöscht, und der Speicherplatz, den sie für den Bucket verwendet haben, wird freigegeben.

Beschränkungen für mehrteilige Uploads von Amazon Simple Storage Service

Die folgende Tabelle enthält die Core-Spezifikationen für den mehrteiligen Upload.

- Maximale Objektgröße: 5 TB
- Maximale Anzahl von Teilen pro Upload: 10 000
- Teilenummern: 1-10.000 (inklusive)
- Teilegröße: 5 MB (Minimum) - 5 GB (Maximum). Es gibt keine Größenbeschränkung für den letzten Teil Ihres mehrteiligen Uploads.
- Maximale Anzahl der zurückgegebenen Teile bei einer Anforderung zum Auflisten der Teile: 1 000
- Maximale Anzahl der zurückgegebenen mehrteiligen Uploads bei einer Anforderung zum Auflisten mehrteiliger Uploads: 1 000

Aufteilen der Datei zum Hochladen

Verwenden der`split`auf dem Linux- oder Unix-Betriebssystem verwenden, um eine Datei in mehrere Teile zu teilen, die Sie dann in Ihren Bucket hochladen. Es gibt ähnliche Free-Ware-Anwendungen, die Sie auf dem Windows-Betriebssystem verwenden können, um eine Datei zu teilen. Nachdem Sie die Datei in mehrere Teile aufgeteilt haben, fahren Sie fort mit dem Abschnitt Starten eines mehrteiligen Uploadsin diesem Leitfaden .

Starten eines mehrteiligen Uploads mit der AWS CLI

Führen Sie das folgende Verfahren aus, um einen mehrteiligen Upload mithilfe der AWS Command Line Interface (AWS CLI) zu starten. Führen Sie dazu den Befehl `create-multipart-upload` aus. Weitere Informationen finden Sie unter create-multipart-upload in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.

2. Geben Sie den folgenden Befehl ein, um einen mehrteiligen Upload für den Bucket zu erstellen.

```
aws s3api create-multipart-upload --bucket BucketName --key ObjectKey --acl bucket-owner-full-control
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *Bucket-Name*- der Name des Buckets, für den Sie einen mehrteiligen Upload erstellen möchten.
- *ObjectKey*- Der Objektschlüssel, der für die Datei verwendet werden soll, die Sie hochladen.

Beispiel:

```
aws s3api create-multipart-upload --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4 --acl bucket-owner-full-control
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten: Die Antwort enthält einen`UploadID`Geben Sie in folgenden Befehlen ein, um Teile hochzuladen und den mehrteiligen Upload für dieses Objekt fertigzustellen.

```
C:\ >aws s3api create-multipart-upload --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4
{
    "AbortDate": "2021-05-20T00:00:00+00:00",
    "AbortRuleId": "ExpireMultiPart",
    "ServerSideEncryption": "AES256",
    "Bucket": "DOC-EXAMPLE-BUCKET",
    "Key": "sailbot.mp4",
    "UploadId": "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.DlHYOTsITFsX.tO3XOUTTAHiCxY5VR8jWRGdkVkUG"
}
```

Nachdem Sie die `UploadID` für Ihren mehrteiligen Upload erhalten haben, fahren Sie fort mit den folgenden Abschnitt Hochladen eines Teils mit der AWS CLI dieses Leitfadens und beginnen Sie mit dem Hochladen von Teilen.

Hochladen eines Teils mit der AWS CLI

Führen Sie das folgende Verfahren aus, um einen Teil eines mehrteiligen Uploads mithilfe der AWS Command Line Interface (AWS CLI) zu starten. Führen Sie dazu den Befehl `upload-part` aus. Weitere Informationen finden unter upload-part in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um ein, um ein Teil in den Bucket hochzuladen.

```
aws s3api upload-part --bucket BucketName --key ObjectKey --part-number Number --
body FilePart --upload-id "UploadID"  --acl bucket-owner-full-control
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *Bucket-Name*- der Name des Buckets, für den Sie einen mehrteiligen Upload erstellen möchten.
- *ObjectKey*- Der Objektschlüssel, der für die Datei verwendet werden soll, die Sie hochladen.
- *Zahl*- Die Teilenummer des Teils, das Sie hochladen. Die Teilenummer identifiziert eindeutig einen Teil und seine Position im Objekt, das Sie hochladen. Bestätigen Sie, dass Sie die`--part-number`-Parameter mit jedem hochgeladenen Teil. Dazu nummerieren Sie sie in der Reihenfolge, in der Amazon Simple Storage Service das Objekt zusammenstellen soll, wenn Sie den mehrteiligen Upload abschließen.
- *FilePart*- Die Teiledatei, die von Ihrem Computer hochgeladen werden soll.
- *UploaDID* – Die Upload-ID des mehrteiligen Uploads, den Sie zuvor in diesem Leitfaden erstellt haben.

Beispiel:

```
aws s3api upload-part --bucket DOC-EXAMPLE-BUCKET --
key sailbot.mp4 --part-number 1 --body sailbot.mp4.001 --upload-id
 "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.Dl
 --acl bucket-owner-full-control
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten: Wiederholen Sie die`upload-part`-Befehl für jedes hochgeladene Teil. Die Antwort für jede Ihrer Upload-Teilanfragen enthält

eineETag-Wert für das hochgeladene Teil. Zeichnen Sie dieETag-Werte für jedes der Teile, die Sie hochladen. Sie benötigen alle ETag-Werte, um den mehrteiligen Upload fertigzustellen, der später in diesem Leitfaden behandelt wird.

```
C:\ >aws s3api upload-part --bucket DOC-EXAMPLE-BUCKET  --key sailbot.mp4  --part-number 1 --body sailbot.mp4.001
 --upload-id "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.DlHYOTsITFsX.tO3XOUTTAHiCxY5VR8jWRGdkVkUG"
{
    "ServerSideEncryption": "AES256",
    "ETag": "\"4example7530246113e837a860a38bbb\""
}
```

Auflisten von Teilen eines mehrteiligen Uploads mit der AWS CLI

Führen Sie das folgende Verfahren vollständig aus, um einen Teil eines mehrteiligen Uploads mithilfe der AWS Command Line Interface (AWS CLI) zu starten. Führen Sie dazu den Befehl `list-parts` aus. Weitere Informationen finden unter list-parts in der AWS CLI-Befehlsreferenz.

Führen Sie dieses Verfahren aus, um dieETag-Werte für alle hochgeladenen Teile in einem mehrteiligen Upload. Sie benötigen diese Werte, um den mehrteiligen Upload abschließen zu können. Wenn Sie jedoch alleETag-Werte aus der Antwort Ihrer Teile-Uploads verwenden, können Sie diese Prozedur überspringen und mit derErstellen eines mehrteiligen Uploads .json-Abschnitt in diesem Dokument.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um die Teile eines mehrteiligen Uploads in Ihrem Bucket aufzulisten.

   ```
   aws s3api list-parts --bucket BucketName --key ObjectKey --upload-id "UploadID"
   ```

   Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

   - *Bucket-Name*- der Name des Buckets, für den Sie die Teile eines mehrteiligen Uploads auflisten möchten.

- *ObjectKey*- Der Objektschlüssel des mehrteiligen Uploads.
- *UploaDID* – Die Upload-ID des mehrteiligen Uploads, den Sie zuvor in diesem Leitfaden erstellt haben.

Beispiel:

```
aws s3api list-parts --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4 --upload-id
 "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.Dl
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten: Die Antwort listet alle Teilenummern undETag-Werte für die Teile, die Sie beim mehrteiligen Upload hochgeladen haben. Kopieren Sie diese Werte in die Zwischenablage, und fahren Sie fort mit dem Abschnitt Erstellen eines mehrteiligen Uploads .json in diesem Leitfaden .

Erstellen eines mehrteiligen Uploads .json

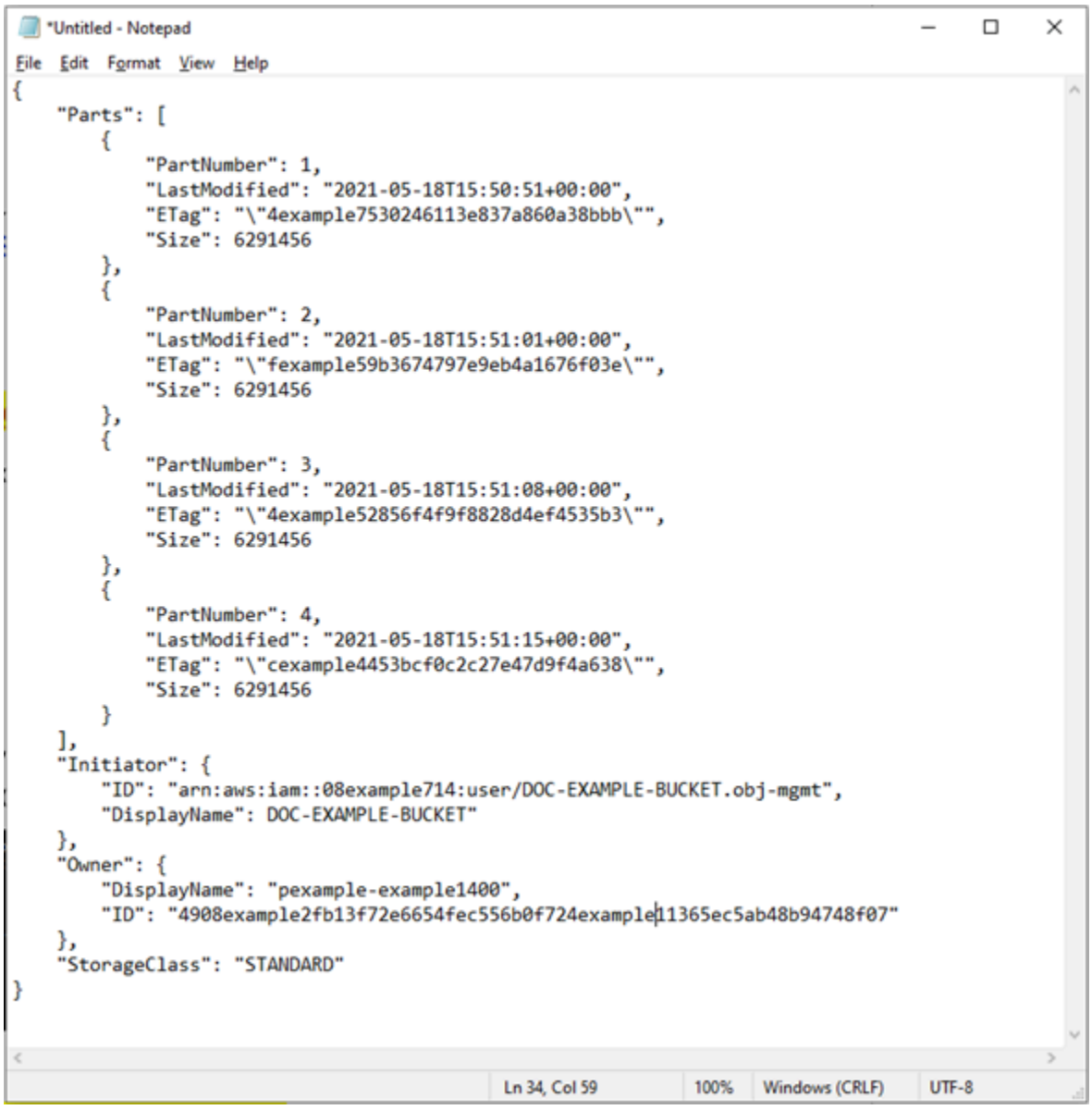

```
C:\>aws s3api list-parts --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4 --upload-id "R4QU.mO.exampleiHWiLOeNw7JtXX7OotR
hTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.DlHYOTsITFsX.tO3XOUTTAHiCxY5VR8jWRGdkVkUG"
{
    "Parts": [
        {
            "PartNumber": 1,
            "LastModified": "2021-05-18T15:50:51+00:00",
            "ETag": "\"4example7530246113e837a860a38bbb\"",
            "Size": 6291456
        },
        {
            "PartNumber": 2,
            "LastModified": "2021-05-18T15:51:01+00:00",
            "ETag": "\"fexample59b3674797e9eb4a1676f03e\"",
            "Size": 6291456
        },
        {
            "PartNumber": 3,
            "LastModified": "2021-05-18T15:51:08+00:00",
            "ETag": "\"4example52856f4f9f8828d4ef4535b3\"",
            "Size": 6291456
        },
        {
            "PartNumber": 4,
            "LastModified": "2021-05-18T15:51:15+00:00",
            "ETag": "\"cexample4453bcf0c2c27e47d9f4a638\"",
            "Size": 6291456
        }
    ],
    "Initiator": {
        "ID": "arn:aws:iam::08example714:user/DOC-EXAMPLE-BUCKET.obj-mgmt",
        "DisplayName": "DOC-EXAMPLE-BUCKET"
    },
    "Owner": {
        "DisplayName": "pexample-example1400",
        "ID": "4908example2fb13f72e6654fec556b0f724example11365ec5ab48b94748f07"
    },
    "StorageClass": "STANDARD"
}
```

Erstellen einer mehrteiligen Upload.json-Datei

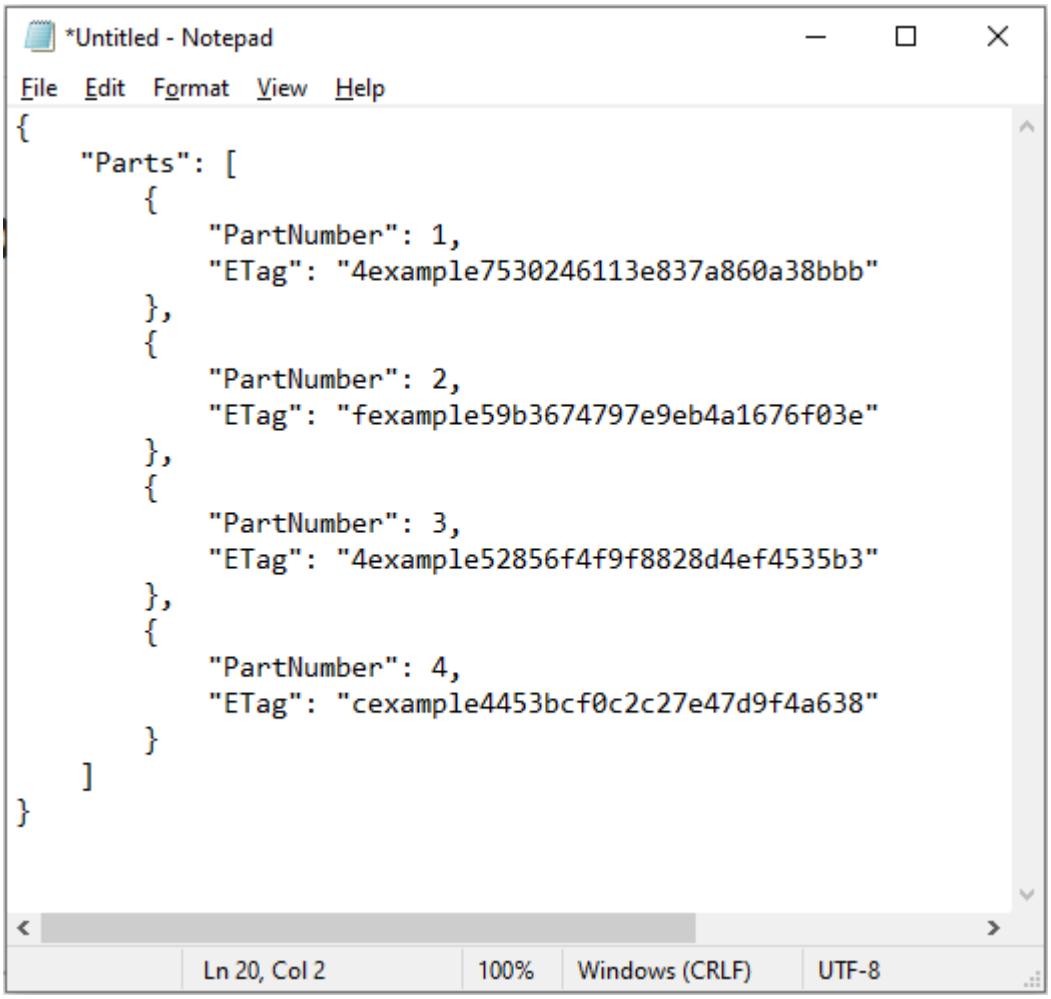
Führen Sie das folgende Verfahren aus, um eine mehrteilige Upload-JSON-Datei zu erstellen, die alle hochgeladenen Teile und deren`ETag`-Werte angeben. Um den mehrteiligen Upload fertigzustellen, ist dies weiter unten in diesem Leitfaden erforderlich.

1. Öffnen Sie einen Text-Editor und fügen Sie die Antwort aus dem `list-parts`-Befehl ein, den Sie im vorherigen Abschnitt dieses Leitfadens angefordert haben.

   Das Ergebnis sollte wie folgt aussehen:



2. Formatieren Sie die Textdatei wie im folgenden Beispiel gezeigt:



3. Speichern Sie die Textdatei auf Ihrem Computer unter `mpstructure.json` und fahren Sie fort zum Abschnitt Abschließen eines mehrteiligen Upload mit der AWS CLI diesem Leitfaden.

Abschließen eines mehrteiligen Upload mit der AWS CLI

Führen Sie das folgende Verfahren vollständig aus, um einen mehrteiligen Upload mithilfe der AWS Command Line Interface (AWS CLI) zu starten. Führen Sie dazu den Befehl `complete-multipart-upload` aus. Weitere Informationen finden Sie unter complete-multipart-upload in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um ein, um ein Teil in den Bucket hochzuladen.

```
aws s3api complete-multipart-upload --multipart-upload file://JSONFileName --
bucket BucketName --key ObjectKey --upload-id "UploadID"  --acl bucket-owner-full-
control
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *JSONFileName* – Der Name der JSON-Datei, die Sie zuvor in diesem Leitfaden erstellt haben (zum Beispiel `mpstructure.json`).
- *Bucket-Name*- der Name des Buckets, für den Sie einen mehrteiligen Upload abschließen möchten.
- *ObjectKey*- Der Objektschlüssel des mehrteiligen Uploads.
- *UploaDID* – Die Upload-ID des mehrteiligen Uploads, den Sie zuvor in diesem Leitfaden erstellt haben.

Example:

```
aws s3api complete-multipart-upload --multipart-upload file://mpstructure.json
 --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4 --upload-id
 "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.Dl
 --acl bucket-owner-full-control
```

Sie sollten eine Reaktion ähnlich dem folgenden Beispiel erhalten. Dadurch wird bestätigt, dass der mehrteilige Upload abgeschlossen ist. Das Objekt ist jetzt zusammengebaut und im Bucket verfügbar.

```
C:\>aws s3api complete-multipart-upload --multipart-upload file://mpstructure.json --bucket DOC-EXAMPLE-BUCKET  --key sailbot.mp4
--upload-id "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.DlHYOTsITFsX.tO3XOUTTAHiCxY5VR8jWRGdkVkUG"
{
    "ServerSideEncryption": "AES256",
    "VersionId": "MexampleKMdfPQb.2YZHqOvE_T.vSDtY",
    "Location": "https://DOC-EXAMPLE-BUCKET.s3.us-west-2.amazonaws.com/sailbot.mp4",
    "Bucket": "DOC-EXAMPLE-BUCKET",
    "Key": "sailbot.mp4",
    "ETag": "\"1example5964e3115e5d3f3c9a731585-4\""
}
```

Auflisten von mehrteiligen Uploads für einen Bucket mit der AWS CLI

Führen Sie das folgende Verfahren vollständig aus, um einen mehrteiligen Upload für einen Bucket über die AWS Command Line Interface (AWS CLI) zu erhalten. Führen Sie dazu den Befehl `list-multipart-uploads` aus. Weitere Informationen finden Sie unter list-multipart-upload in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um ein, um ein Teil in den Bucket hochzuladen.

   ```
   aws s3api list-multipart-uploads --bucket BucketName
   ```

   Ersetzen Sie im Befehl*Bucket-Name*mit dem Namen des Buckets, für den Sie alle mehrteilige Uploads auflisten möchten.

   Beispiel:

   ```
   aws s3api list-multipart-uploads --bucket DOC-EXAMPLE-BUCKET
   ```

   Sie sollten eine Reaktion ähnlich dem folgenden Beispiel erhalten.

   ```
   C:\>aws s3api list-multipart-uploads --bucket DOC-EXAMPLE-BUCKET
   {
       "Uploads": [
           {
               "UploadId": "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.DlHYOTsITFsX.tO3XOUTTAHiCxY5VR8jWRGdkVkUG",
               "Key": "sailbot.mp4",
               "Initiated": "2021-05-18T15:49:11+00:00",
               "StorageClass": "STANDARD",
               "Owner": {
                   "DisplayName": "pexample-example1400",
                   "ID": "4908example2fb13f72e6654fec556b0f724example11365ec5ab48b94748f07"
               },
               "Initiator": {
                   "ID": "arn:aws:iam::08example714:user/DOC-EXAMPLE-BUCKET.obj-mgmt",
                   "DisplayName": "DOC-EXAMPLE-BUCKET"
               }
           }
       ]
   }
   ```

Auflisten von mehrteiligen Uploads mit der AWS CLI

Führen Sie das folgende Verfahren aus, um einen mehrteiligen Upload über die AWS Command Line Interface (AWS CLI) zu erhalten. Sie tun dies, wenn Sie einen mehrteiligen Upload gestartet haben, ihn aber nicht mehr fortsetzen möchten. Führen Sie dazu den Befehl `abort-multipart-upload` aus. Weitere Informationen finden Sie unter abort-multipart-upload in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um ein, um ein Teil in den Bucket hochzuladen.

```
aws s3api abort-multipart-upload --bucket BucketName --key ObjectKey --upload-id
 "UploadID" --acl bucket-owner-full-control
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *Bucket-Name*- der Name des Buckets, für den Sie einen mehrteiligen Upload abbrechen möchten.
- *ObjectKey*- Der Objektschlüssel des mehrteiligen Uploads.
- *UploaDID*- Die Upload-ID des mehrteiligen Uploads, den Sie stoppen möchten.

Beispiel:

```
aws s3api abort-multipart-upload --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4 --
upload-id
 "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.Dl
 --acl bucket-owner-full-control
```

Der Befehl gibt keine Antwort zurück. Sie können einen`list-multipart-uploads`, um zu bestätigen, dass der mehrteilige Upload beendet wurde.

Regeln für die Benennung von Buckets in Amazon Lightsail

Wenn Sie einen Bucket in der Amazon Lightsail-Objektspeicherkennung verwenden, müssen Sie ihr einen Namen geben. Der Name des Buckets ist Teil der URL, die Ihre Kunden beim Zugriff auf Objekte verwenden, die im Bucket gespeichert sind. Wenn Sie beispielsweise Ihren Bucket in der `us-east-1` AWS-Region `DOC-EXAMPLE-BUCKET` benennen, lautet die URL für Ihren Bucket `DOC-EXAMPLE-BUCKET.s3.us-east-1.amazonaws.com`. Sobald Ihr Bucket erstellt ist, kann der Name nicht mehr geändert werden. Beachten Sie, dass Ihre Kunden den von Ihnen angegebenen Bucket-Namen sehen können. Weitere Informationen zu Lightsail-Objektspeicherservice finden Sie unter Objektspeicher. Weitere Informationen zum Erstellen eines Buckets finden Sie unter Erstellen eines Buckets.

Bucket-Namen müssen DNS-konform sein. Aus diesem Grund gelten die folgenden Regeln für die Benennung von Buckets in Lightsail:

- Bucket-Namen dürfen zwischen 3 und 56 Zeichen betragen.
- Bucket-Namen können nur aus Kleinbuchstaben, Zahlen und Bindestrichen (-) bestehen.
- Bucket-Namen müssen mit einem Buchstaben oder einer Zahl beginnen und enden.
- Bindestriche (-) können Wörter trennen, können aber nicht nacheinander angegeben werden. `doc-example-bucket` ist beispielsweise zulässig, aber `doc--example--bucket` ist es nicht.
- Bucket-Namen müssen innerhalb der `aws`-Partition (Standardregionen), einschließlich Buckets in Amazon Simple Storage Service (Amazon S3), einzigartig sein.

Bucket-Beispielnamen

Die folgenden Beispielnamen für Buckets sind gültig und folgen den empfohlenen Benennungsrichtlinien:

- `docexamplebucket1`
- `log-delivery-march-2020`
- `my-hosted-content`

Die folgenden Beispiel-Bucket-Namen sind nicht erlaubt:

- `doc.example.bucket`

- `doc--example--bucket`
- `doc-example-bucket-`

Schlüsselnamen für Lightsail-Objektspeicher-Buckets

Dateien, die Sie in Ihren Bucket hochladen, werden als Objekte im Amazon Lightsail-Objektspeicherservice gespeichert. Der Objektschlüssel (oder Schlüsselname) identifiziert das Objekt in einem Bucket eindeutig. In diesem Handbuch wird das Konzept der Schlüsselnamen und Schlüsselnamenpräfixe erläutert, die die Ordnerstruktur von Buckets bilden, die über die Lightsail-Konsole angezeigt werden. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Schlüsselnamen

Das Datenmodell des Lightsail-Objektspeicherdienstes verwendet eine flache Struktur anstelle einer hierarchischen Struktur, wie Sie sie in einem Dateisystem sehen würden. Es gibt keine Hierarchie von Ordnern und Unterordnern. Sie können jedoch mit den Schlüsselnamenpräfixen und Trennzeichen eine logische Hierarchie erschließen, wie dies die -Konsole tut. Die Lightsail-Konsole verwendet die Schlüsselnamenpräfixe, um Ihre Objekte in einer Ordnerstruktur anzuzeigen.

Angenommen, Ihr Bucket () enthält vier Objekte mit den folgenden Objektschlüsseln:

- `Development/Projects.xls`
- `Finance/statement1.pdf`
- `Private/taxdocument.pdf`
- `to-dos.doc`

Die Lightsail-Konsole verwendet die Schlüsselnamenpräfixe (`Development/Finance/`, und`Private/`) und das Trennzeichen (`/`), um eine Ordnerstruktur darzustellen. Der `to-dos.doc`-Schlüssel hat kein Präfix, deshalb erscheint sein Objekt direkt auf Root-Ebene des Buckets. Wenn Sie in der Lightsail-Konsole zu dem `Development/` Ordner wechseln, sehen Sie das `Projects.xls` Objekt. Im Ordner `Finance/`, wird das `statement1.pdf`-Objekt angezeigt; und im Ordner `Private/`, wird das`taxdocument.pdf`-Objekt angezeigt.

Die Lightsail-Konsole ermöglicht die Ordnererstellung, indem ein Null-Byte-Objekt mit dem Schlüsselnamenpräfix und dem Trennzeichenwert als Schlüsselname erstellt wird. Diese Ordnerobjekte werden nicht in der Konsole angezeigt. Sie verhalten sich jedoch wie alle anderen

Objekte. Sie können sie mithilfe der Amazon S3 S3-API, AWS Command Line Interface (AWS CLI) oder AWS SDKs anzeigen und bearbeiten.

Richtlinien für Objektschlüsselnamen

Sie können in einem Objektschlüsselnamen jedes beliebige UTF-8-Zeichen verwenden. Die Verwendung bestimmter Zeichen in Schlüsselnamen kann jedoch bei manchen Anwendungen und Protokollen zu Problemen führen. Die folgenden Richtlinien helfen Ihnen, die Compliance mit DNS, web-sicheren Zeichen, XML-Parsern und anderen APIs zu maximieren.

Sichere Zeichen

Die folgenden Zeichensätze sind allgemein sicher für die Verwendung in Schlüsselnamen.

- Alphanumerische Zeichen
  - 0-9
  - a-z
  - A-Z
- Sonderzeichen
  - Schrägstrich (`/`)
  - Ausrufezeichen (`!`)
  - Bindestrich (`-`)
  - Unterstrich (`_`)
  - Punkt (`.`)
  - Sternchen (`*`)
  - Einzelnes Anführungszeichen (`'`)
  - Öffnende Klammer (`(`)
  - Schließende Klammer (`)`)

Nachfolgend finden Sie Beispiele für gültige Objektschlüsselnamen:

- `4my-organization`
- `my.great_photos-2014/jan/myvacation.jpg`
- `videos/2014/birthday/video1.wmv`

> **Important**
>
> Wenn ein Objektschlüsselname mit einem einzigen Punkt (.) oder zwei Punkten (..) endet, können Sie das Objekt nicht mit der Lightsail-Konsole herunterladen. Um ein Objekt herunterzuladen, dessen Schlüsselname mit einem oder zwei Punkten endet, müssen Sie die Amazon S3 S3-API und die AWS SDKs verwenden. AWS CLI Weitere Informationen finden Sie unter Herunterladen von Objekten aus einem Bucket.

Zeichen, die möglicherweise eine Sonderverarbeitung benötigen

Die folgenden Zeichen in einem Schlüsselnamen erfordern möglicherweise eine zusätzliche Verarbeitung im Code oder müssen URL-codiert oder als HEX angegeben werden. Einige davon sind nicht darstellbare Zeichen, und Ihr Browser kann sie ggf. nicht verarbeiten, was zudem einer speziellen Vorgehensweise bedarf:

- Ampersand ("&")
- Dollar ("$")
- ASCII-Zeichenbereiche 00–1F hex (0–31 dezimal) und 7F (127 dezimal)
- 'At'-Symbol ("@")
- Gleichheitszeichen ("=")
- Semikolon (";")
- Doppelpunkt (":")
- Plus ("+")
- Leerzeichen – Wichtige Leerzeichenfolgen gehen möglicherweise bei bestimmten Verwendungszwecken verloren (insbesondere Mehrfachleerzeichen).
- Komma (",")
- Fragezeichen ("?")

Zeichen, die Sie vermeiden sollten

Sie sollten in Schlüsselnamen die folgenden Zeichen vermeiden, weil sie einen maßgeblichen Arbeitsaufwand erfordern, um konsistent über alle Anwendungen zu sein.

- Umgekehrter Schrägstrich ("\")

- Linke geschweifte Klammer ("{")
- Nicht darstellbare ASCII-Zeichen (128-255 Dezimalzeichen)
- Caret ("^")
- Rechte geschweifte Klammer ("}")
- Prozentzeichen ("%")
- Accent Grave ("`")
- Rechte eckige Klammer ("]")
- Anführungszeichen
- Größersymbol (">")
- Linke eckige Klammer ("[")
- Tilde ("~")
- Kleiner als-Zeichen ("<")
- Pfundzeichen ("#")
- Vertikaler Strich ("|")

Schlüsselbeschränkungen für XML-bezogene Objekte

Gemäß dem XML-Standard für die end-of-line Verarbeitung ist der gesamte XML-Text normalisiert, sodass Zeilenumbrüche (ASCII-Code 13) und Zeilenumbrüche, denen unmittelbar ein Zeilenvorschub folgt (ASCII-Code 10), durch ein einzelnes Zeilenvorschubzeichen ersetzt werden. Um das korrekte Parsen von Objektschlüsseln in XML-Anforderungen zu gewährleisten, müssen Zeilenumbrüche und andere Sonderzeichen durch den entsprechenden XML-Entitätscode ersetzt werden, wenn sie in XML-Markierungen eingefügt werden. Im Folgenden finden Sie eine Liste solcher Sonderzeichen und ihrer entsprechenden Entitätscodes:

- ' wie `'`
- ” wie `"`
- & wie `&`
- < wie `<`
- < wie `>`
- `\r` als `
` oder`
`
- `\n` als `
` oder`
`

Das folgende Beispiel veranschaulicht die Verwendung eines XML-Entitätscodes als Ersatz für eine Zeilenumschaltung. Diese `DeleteObjects`-Anforderung löscht ein Objekt mit dem -Parameter/`some/prefix/objectwith\rcarriagereturn` (wobei\ r die Zeilenumschaltung ist).

```
<Delete xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
      <Object>
        <Key>/some/prefix/objectwith&#13;carriagereturn</Key>
      </Object>
    </Delete>
```

Bewährte Sicherheitsmethoden für Objektspeicher in Lightsail

Amazon Lightsail Objektspeicher enthält eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Inhalt

- Überwachen von AWS-Sicherheitsempfehlungen

Bewährte Methoden für vorbeugende Sicherheitsmaßnahmen

Die folgenden bewährten Methoden können dazu beitragen, Sicherheitsvorfälle mit Lightsail-Buckets zu verhindern.

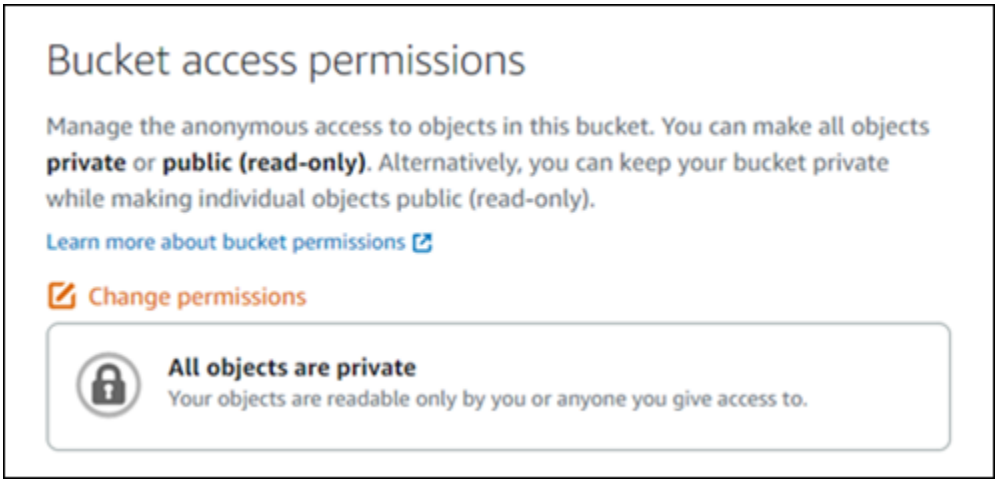
Implementieren des Zugriffs mit geringsten Berechtigungen

Beim Erteilen von Berechtigungen entscheiden Sie, wer welche Berechtigungen für welche Lightsail-Ressourcen erhält. Sie aktivieren die spezifischen Aktionen, die daraufhin für die betreffenden Ressourcen erlaubt sein sollen. Aus diesem Grund sollten Sie nur Berechtigungen gewähren, die zum Ausführen einer Aufgabe erforderlich sind. Die Implementierung der geringstmöglichen Zugriffsrechte ist eine grundlegende Voraussetzung zum Reduzieren des Sicherheitsrisikos und der Auswirkungen, die aufgrund von Fehlern oder böswilligen Absichten entstehen könnten.

Weitere Informationen zum Erstellen einer IAM-Richtlinie zum Verwalten von Buckets finden Sie unter IAM-Richtlinie zum Verwalten von Buckets. Weitere Informationen zu den von Lightsail-Buckets unterstützten Amazon-S3-Aktionen finden Sie unter Aktionen für die Objektspeicherung in der Amazon Lightsail-API-Referenz.

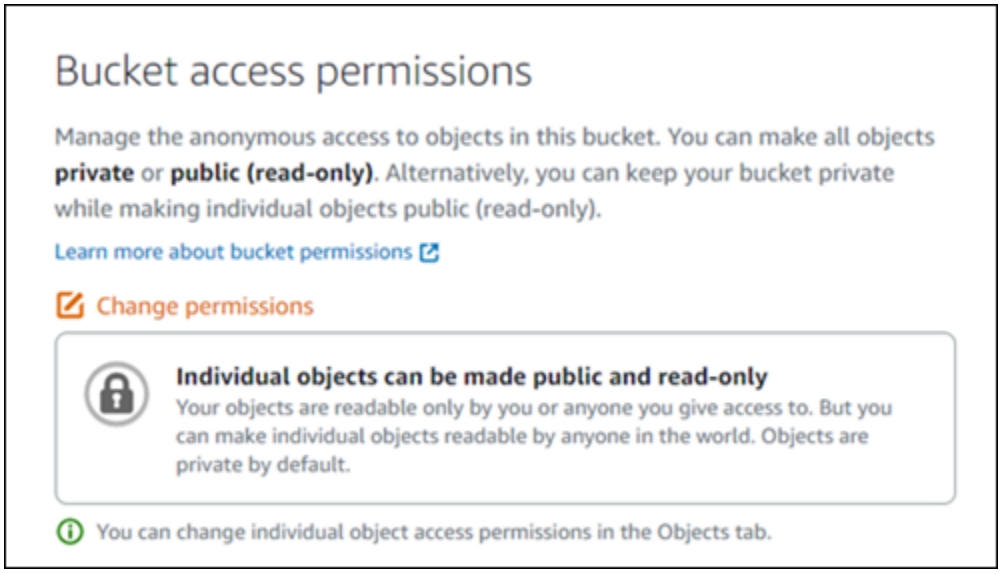
Sicherstellen, dass Ihre Lightsail-Buckets nicht öffentlich zugänglich sind

Buckets und Objekte sind standardmäßig privat. Halten Sie Ihren Bucket privat, indem Sie die Bucket-Zugriffsberechtigung auf All objects are private (Alle Objekte sind privat) setzen. In den meisten Anwendungsfällen müssen Sie Ihren Bucket oder einzelne Objekte nicht öffentlich machen. Weitere Informationen finden Sie unter Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket.

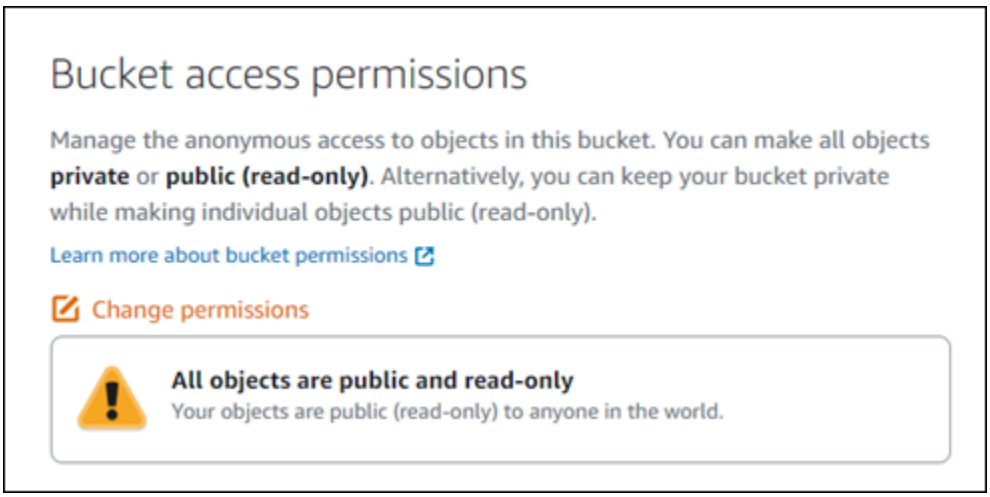


Wenn Sie jedoch Ihren Bucket verwenden, um Medien für Ihre Website oder Anwendung zu hosten, müssen Sie in bestimmten Szenarien möglicherweise Ihren Bucket oder einzelne Objekte öffentlich machen. Sie können eine der folgenden Optionen konfigurieren, um Ihren Bucket oder einzelne Objekte öffentlich zu machen:

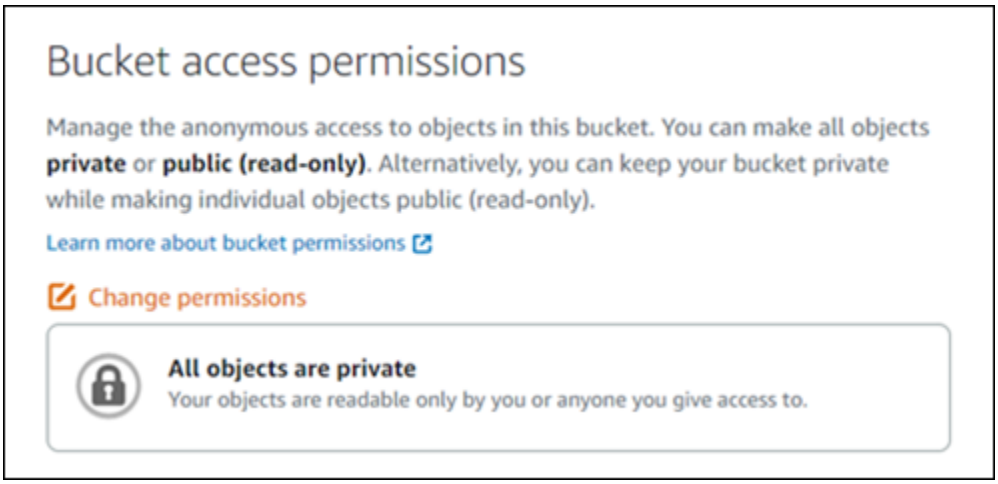
- Wenn nur einige der Objekte in einem Bucket für jeden im Internet öffentlich (schreibgeschützt) sein müssen, ändern Sie die Bucket-Zugriffsberechtigung in Einzelne Objekte können öffentlich und schreibgeschützt gemacht werden und ändern Sie nur die Objekte, die öffentlich sein müssen in Öffentlich (schreibgeschützt). Diese Option hält den Bucket privat, gibt Ihnen jedoch die Möglichkeit, einzelne Objekte öffentlich zu machen. Machen Sie ein einzelnes Objekt nicht öffentlich, wenn es sensible oder vertrauliche Informationen enthält, die nicht öffentlich zugänglich sein sollen. Wenn Sie einzelne Objekte öffentlich machen, sollten Sie die öffentliche Zugänglichkeit jedes einzelnen Objekts regelmäßig überprüfen.



- Wenn alle Objekte im Bucket für jeden im Internet öffentlich (schreibgeschützt) sein müssen, ändern Sie die Bucket-Zugriffsberechtigung in Alle Objekte sind öffentlich und schreibgeschützt. Verwenden Sie diese Option nicht, wenn eines Ihrer Objekte im Bucket sensible oder vertrauliche Informationen enthält.



- Wenn Sie zuvor einen Bucket in öffentlich oder einzelne Objekte in öffentlich geändert haben, können Sie den Bucket und alle seine Objekte schnell in privat ändern, indem Sie die Bucket-Zugriffsberechtigung in All objects are private (Alle Objekte sind privat) ändern.

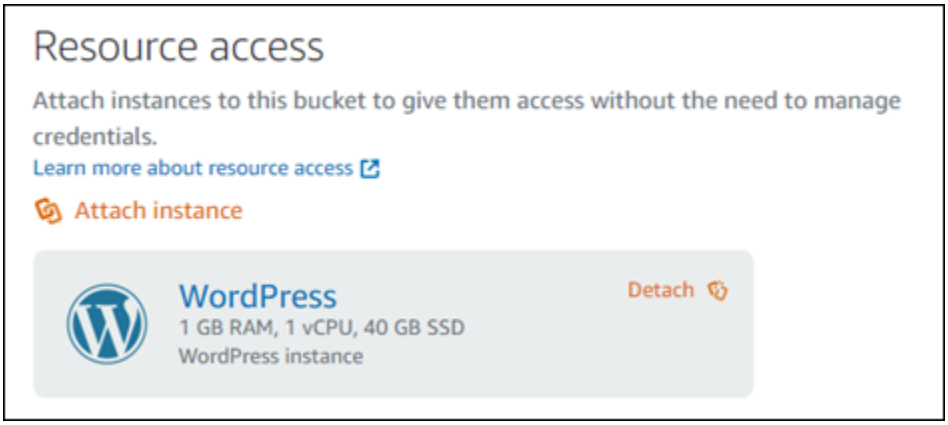


Blockieren des öffentlichen Zugriffs in Amazon S3 aktivieren

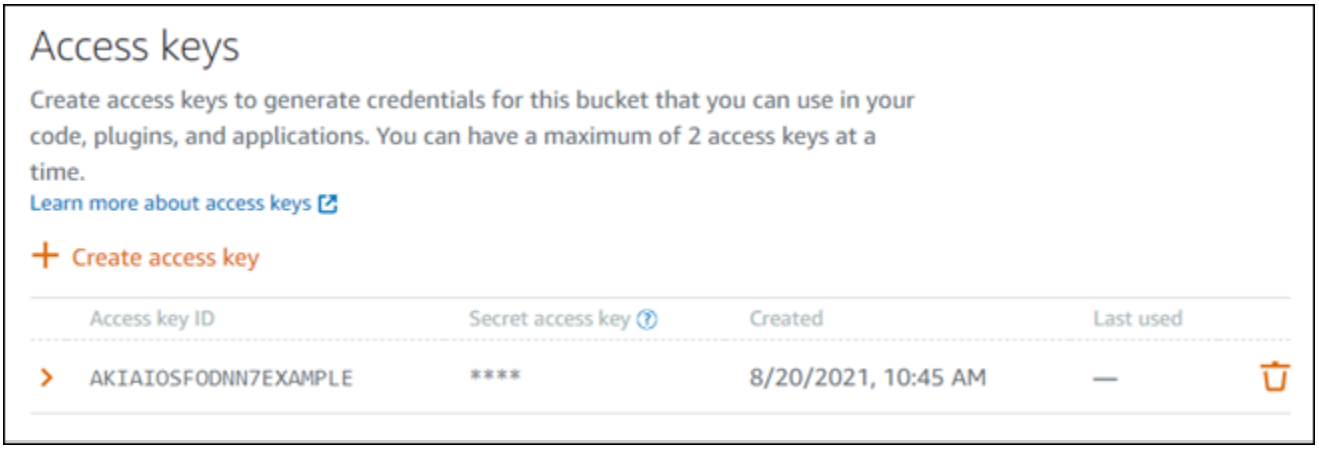
Lightsail-Objektspeicherressourcen berücksichtigen sowohl Lightsail-Bucket-Zugriffsberechtigungen als auch Amazon-S3-Konfigurationen zum Blockieren des öffentlichen Zugriffs auf Kontoebene, wenn Sie den öffentlichen Zugriff zulassen oder verweigern. Mit der Funktion zum Blockieren des öffentlichen Zugriffs auf Kontoebene in Amazon S3 können Kontoadministratoren und Bucket-Eigentümer den öffentlichen Zugriff auf ihre Amazon-S3- und Lightsail-Buckets beschränken. Blockieren des öffentlichen Zugriffs kann alle Amazon-S3- und Lightsail-Buckets privat machen, unabhängig davon, wie die Ressourcen erstellt wurden, und unabhängig von den einzelnen Bucket- und Objektberechtigungen, die möglicherweise konfiguriert wurden. Weitere Informationen finden Sie unter Blockieren des öffentlichen Zugriffs für Buckets.

Anhängen von Instances an Buckets, um vollständigen programmatischen Zugriff zu gewähren

Das Anhängen einer Instance an einen Lightsail-Objektspeicher-Bucket ist die sicherste Methode, um Zugriff auf den Bucket bereitzustellen. Die Resource access (Ressourcenzugriff) Funktion, mit der Sie eine Instance an einen Bucket anhängen, gewährt der Instance vollen programmatischen Zugriff auf den Bucket. Mit dieser Methode müssen Sie Bucket-Anmeldeinformationen nicht direkt in der Instance oder Anwendung speichern und Sie müssen die Anmeldeinformationen nicht regelmäßig drehen. Zum Beispiel können einige WordPress-Plug-Ins auf einen Bucket zugreifen, auf den die Instance Zugriff hat. Weitere Informationen finden Sie unter Konfigurieren des Ressourcenzugriffs für einen Bucket und Tutorial: Verbinden Ihrer WordPress-Instance mit einem Bucket.



Wenn sich die Anwendung jedoch nicht auf einer Lightsail-Instance befindet, können Sie Bucket-Zugriffsschlüssel erstellen und konfigurieren. Bucket-Zugriffsschlüssel sind langfristige Anmeldeinformationen, die nicht automatisch gedreht werden.



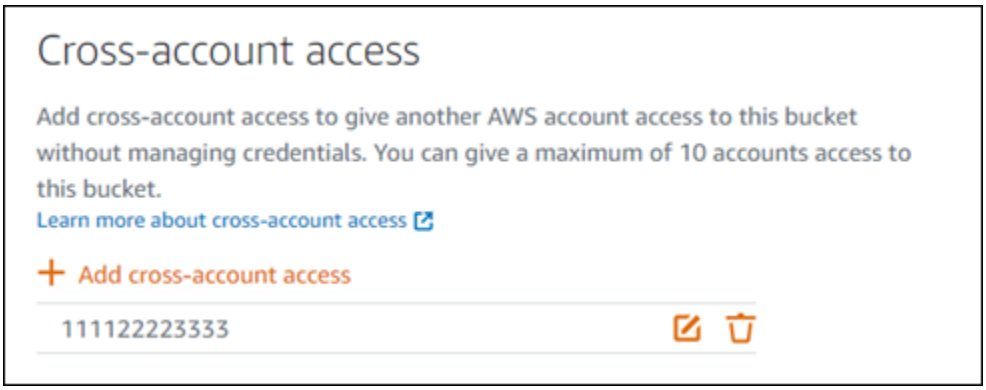
Sie können Zugriffsschlüssel erstellen und verwenden, um Anwendungen oder Plug-Ins vollen programmatischen Zugriff auf Objekte in Ihrem Bucket zu gewähren. Wenn Sie einen Zugriffsschlüssel mit Ihrem Bucket verwenden, sollten Sie Ihre Schlüssel regelmäßig drehen und

eine Bestandsaufnahme der vorhandenen Schlüssel machen. Bestätigen Sie, dass das Datum, an dem ein Zugriffsschlüssel zuletzt verwendet wurde, und die AWS-Region, in der er verwendet wurde, Ihren Erwartungen entspricht, wie der Schlüssel verwendet werden sollte. Das Datum, an dem ein Zugriffsschlüssel zuletzt verwendet wurde, wird in der Lightsail-Konsole angezeigt; im Abschnitt Access key (Zugriffsschlüssel) der Registerkarte Berechtigungen der Verwaltungsseite eines Buckets. Löschen Sie Zugriffsschlüssel, die nicht verwendet werden.

Wenn Sie Ihren geheimen Zugriffsschlüssel versehentlich mit der Öffentlichkeit teilen, sollten Sie ihn löschen und einen neuen erstellen. Sie können maximal zwei Zugriffsschlüssel pro Bucket besitzen. Obwohl Sie zwei verschiedene Zugriffsschlüssel gleichzeitig haben können, ist es hilfreich, einen Zugriffsschlüssel in Ihrem Bucket nicht zu verwenden, wenn Sie einen Schlüssel mit minimalen Ausfallzeiten drehen müssen. Um einen Zugriffsschlüssel zu drehen, erstellen Sie einen neuen, konfigurieren Sie ihn in Ihrer Software und testen Sie ihn. Löschen Sie dann den vorherigen Schlüssel. Das Löschen eines Zugriffsschlüssels ist ein endgültiger Vorgang, der nicht rückgängig gemacht werden kann. Er kann nur durch einen neuen Zugriffsschlüssel ersetzt werden. Weitere Informationen finden Sie unter Erstellen von Bucket-Zugriffsschlüsseln.

Verwenden von kontoübergreifendem Zugriff, um anderen AWS-Konten Zugriff auf Objekte in Ihrem Bucket zu geben

Sie können den kontoübergreifenden Zugriff verwenden, um Objekte in einem Bucket für eine bestimmte Person zugänglich zu machen, die über ein AWS-Konto verfügt, ohne den Bucket und seine Objekte öffentlich zu machen. Wenn Sie den kontoübergreifenden Zugriff konfiguriert haben, stellen Sie sicher, dass die aufgelisteten Konto-IDs die richtigen Konten sind, denen Sie Zugriff auf Objekte in Ihrem Bucket gewähren möchten. Weitere Informationen finden Sie unter Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket.



Datenverschlüsselung

Lightsail führt serverseitige Verschlüsselung mit von Amazon verwalteten Schlüsseln und Verschlüsselung von Daten während der Übertragung durch, indem HTTPS (TLS) durchgesetzt wird. Die serverseitige Verschlüsselung hilft, das Risiko für Ihre Daten zu reduzieren, indem die Daten mit einem Schlüssel verschlüsselt werden, der in einem separaten Service gespeichert wird. Darüber hinaus trägt die Verschlüsselung von Daten während der Übertragung dazu bei, dass potenzielle Angreifer den Netzwerkverkehr mit Person-in-the-Middle-Angriffen oder ähnlichen Angriffen abhören oder manipulieren können.

Aktivieren von Versioning

Das Versioning ermöglicht Ihnen, mehrere Versionen eines Objekts im selben Bucket aufzubewahren. Sie können Versioning verwenden, um sämtliche Versionen aller Objekte in Ihrem Lightsail Bucket zu speichern, abzurufen oder wiederherzustellen. Daten lassen sich dank Versioning nach unbeabsichtigten Benutzeraktionen und Anwendungsfehlern leicht wiederherstellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen der Bucket-Objekt-Versionsverwaltung.

Bewährte Methoden zur Überwachung und Prüfung

Mithilfe der folgenden bewährten Methoden können Sie potenzielle Sicherheitsschwächen und Vorfälle für Lightsail-Buckets erkennen.

Aktivieren Sie die Zugriffsprotokollierung und führen Sie regelmäßige Sicherheits- und Zugriffsprüfungen durch

Die Zugriffsprotokollierung bietet detaillierte Aufzeichnungen über die Anforderungen, die an einen Bucket gestellt wurden. Dabei kann es sich um den Anforderungstyp (`GET`, `PUT`), die in der Anfrage angegebenen Ressourcen sowie Uhrzeit und Datum der Anfrageverarbeitung handeln. Aktivieren Sie die Zugriffsprotokollierung für einen Bucket und führen Sie regelmäßig eine Sicherheits- und Zugriffsprüfung durch, um die Entitäten zu identifizieren, die auf Ihren Bucket zugreifen. Standardmäßig erfasst Lightsail standardmäßig keine Zugriffsprotokolle für Ihre Buckets. Sie müssen die Zugriffsprotokollierung manuell aktivieren. Weitere Informationen finden Sie unter Bucket-Zugriffsprotokolle und Bucket-Zugriffsprotokollierung aktivieren.

Identifizieren, markieren und prüfen Sie Ihre Lightsail-Buckets

Die Identifikation Ihrer IT-Assets ist ein wichtiger Aspekt von Governance und Sicherheit. Es ist erforderlich, dass Sie alle Ihre Lightsail-Buckets sehen, um ihren Sicherheitsstatus beurteilen und Maßnahmen gegen potenzielle Schwachstellen ergreifen zu können.

Verwenden Sie die Markierung, um sicherheits- und prüfungsrelevante Ressourcen zu identifizieren. Verwenden Sie dann diese Tags zur Suche nach den entsprechenden Ressourcen. Weitere Informationen finden Sie unter Tags.

Implementieren der Überwachung mit AWS-Überwachungstools

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Sicherheit, Verfügbarkeit und Leistung von Lightsail-Buckets und anderen Ressourcen. Sie können Benachrichtigungsalarme für die Bucket-Größe (`BucketSizeBytes`) und`Number of objects` (NumberOfObjects)-Bucket-Metriken in Lightsail überwachen und erstellen. Sie möchten beispielsweise benachrichtigt werden, wenn die Größe Ihres Buckets auf eine bestimmte Größe vergrößert oder verkleinert wird oder wenn die Anzahl der Objekte in Ihrem Bucket auf eine bestimmte Anzahl steigt oder sinkt. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen.

Verwenden von AWS CloudTrail

AWS CloudTrail liefert Aufzeichnungen der Aktionen eines Benutzers, einer Rolle oder eines AWS-Service in Lightsail. Mit den von CloudTrail erfassten Informationen können Sie die an Lightsail gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Angaben bestimmen. Sie können beispielsweise CloudTrail-Einträge für Aktionen identifizieren, die eine Auswirkung auf den Datenzugriff haben, insbesondere `CreateBucketAccessKey`, `GetBucketAccessKeys`, `DeleteBucketAccessKey`, `SetResourceAccessForBucket` und `UpdateBucket`. Wenn Sie Ihr AWS-Konto einrichten, ist CloudTrail standardmäßig aktiviert. Sie können aktuelle Ereignisse in der CloudTrail-Konsole anzeigen. Um eine laufende Aufzeichnung von Aktivitäten und Ereignissen für Ihre Lightsail-Buckets zu erstellen, können Sie einen Pfad (Trail) in der CloudTrail-Konsole erstellen. Weitere Informationen finden Sie unter Protokollierung von Datenereignissen für Trails im AWS CloudTrail-Benutzerhandbuch.

Überwachen von AWS-Sicherheitsempfehlungen

Überwachen Sie aktiv die primäre E-Mail-Adresse, die für Ihr AWS-Konto registriert ist. AWS wird Sie über diese E-Mail-Adresse über neue Sicherheitsprobleme informieren, die Sie betreffen könnten.

Operative AWS-Probleme mit weitreichenden Auswirkungen werden auf dem AWS Service Health Dashboard gepostet. Operative Probleme werden ebenfalls über das Personal Health Dashboard in den einzelnen Konten gepostet. Weitere Informationen finden Sie in der AWS-Zustands-Dokumentation.

Grundlegendes zu Bucket-Berechtigungen inAmazon Lightsail

Standardmäßig sind alle Amazon Lightsail-Objektspeicher-Ressourcen – Buckets und Objekte – privat. Das bedeutet, dass nur der Bucket-Eigentümer, das Lightsail-Konto, das es erstellt hat, auf den Bucket und seine Objekte zugreifen kann. Optional kann der Bucket-Eigentümer auch anderen Zugriff gewähren. Sie können den Zugriff auf einen Bucket und dessen Objekte wie folgt gewähren:

- Schreibgeschützter Zugriff— Die folgenden Optionen steuern den schreibgeschützten Zugriff auf einen Bucket und seine Objekte über die URL des Buckets (z. B.`https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`) enthalten.
  - Zugriffsberechtigungen für Bucket— Verwenden Sie Bucket-Zugriffsberechtigungen, um allen Benutzern im Internet Zugriff auf alle Objekte in einem Bucket zu gewähren. Weitere Informationen finden Sie unter Zugriffsberechtigungen für Bucketweiter unten in diesem Leitfaden.
  - Zugriffsberechtigungen für einzelne Objekte – Verwenden Sie einzelne Objektzugriffsberechtigungen, um jedem Benutzer im Internet Zugriff auf ein einzelnes Objekt in einem Bucket zu gewähren. Weitere Informationen finden Sie unter Zugriffsberechtigungen für einzelne Objekte weiter unten in diesem Leitfaden.
  - Kontenübergreifender Zugriff – Verwenden Sie den kontoübergreifenden Zugriff, um anderen Zugriff auf alle Objekte in einem Bucket für andere AWS-Konten zu gewähren. Weitere Informationen finden Sie unter Kontenübergreifender Zufgriffsschlüssel weiter unten in diesem Leitfaden.
- Lese- und Schreibzugriff— Mit den folgenden Optionen steuern Sie den vollständigen Lese- und Schreibzugriff auf einen Bucket und dessen Objekte. Verwenden Sie diese Optionen mit der AWS Command Line Interface (AWS CLI), AWS-APIs und AWS-SDKs.
  - Access keys (Zugriffsschlüssel) — Verwenden Sie Zugriffsschlüssel, um den Zugriff auf Anwendungen oder Plugins zu gewähren. Weitere Informationen finden Sie unter Access keys (Zugriffsschlüssel) weiter unten in diesem Leitfaden.
  - Resource access (Ressourcenzugriff) Verwenden Sie den Ressourcenzugriff, um Zugriff auf eineLightsail Instance zu gewähren. Weitere Informationen finden Sie unter Resource access (Ressourcenzugriff) weiter unten in diesem Leitfaden.

- Blockieren des öffentlichen Zugriffs in Amazon Simple Storage Service – Benutzen Sie das Feature von Amazon Simple Storage Service (Amazon S3) zum Blockieren des öffentlichen Zugriffs auf Kontoebene, um den öffentlichen Zugriff auf Buckets in Amazon S3 und in Lightsail zentral zu limitieren. Block Public Access kann alle Amazon-S3- und Lightsail-Buckets privat machen, unabhängig von den einzelnen Bucket- und Objektberechtigungen, die möglicherweise konfiguriert wurden. Weitere Informationen finden Sie unter Amazon S3 Block Public Access weiter unten in diesem Leitfaden.

Weitere Informationen zu Buckets finden Sie unter Objektspeicher. Weitere Informationen zu bewährten Methoden für die Sicherheit finden Sie unter Bewährte Methoden für die Sicherheit für Objektspeicher.

Zugriffsberechtigungen für Buckets

Verwenden Sie Bucket-Zugriffsberechtigungen, um den öffentlichen (nicht authentifizierten) schreibgeschützten Zugriff auf Objekte in einem Bucket zu steuern. Sie können beim Konfigurieren von Bucket-Zugriffsberechtigungen für Bucket eine der folgenden Optionen wählen:

- All objects are private (Alle Objekte sind privat) — Alle Objekte im Bucket sind nur von Ihnen oder jedem, auf den Sie Zugriff gewähren, lesbar. Diese Option lässt nicht zu, dass einzelne Objekte öffentlich gemacht werden (schreibgeschützt).
- Einzelne Objekte können öffentlich gemacht werden (schreibgeschützt)— Objekte im Bucket können nur von Ihnen oder jedem Benutzer gelesen werden, auf den Sie Zugriff gewähren, es sei denn, Sie geben ein einzelnes Objekt als öffentlich (schreibgeschützt) an. Mit dieser Option können einzelne Objekte öffentlich gemacht werden (schreibgeschützt). Weitere Informationen finden Sie unter Zugriffsberechtigungen für einzelne Objekte weiter unten in diesem Leitfaden.
- Alle Objekte sind öffentlich (schreibgeschützt)— Alle Objekte im Bucket sind für jedermann im Internet lesbar. Alle Objekte im Bucket werden von jedermann im Internet über die URL des Buckets lesbar (z. B.`https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`), wenn Sie diese Option auswählen.

Weitere Informationen zum Konfigurieren von Bucket-Zugriffsberechtigungen finden Sie unter Konfigurieren von Zugriffsberechtigungen für Buckets.

Zugriffsberechtigung für einzelne Objekte

Verwenden Sie Zugriffsberechtigungen für einzelne Objekte, um den öffentlichen (nicht authentifizierten) schreibgeschützten Zugriff auf einzelne Objekte in einem Bucket zu steuern. Zugriffsberechtigungen für einzelne Objekte können nur konfiguriert werden, wenn die Zugriffsberechtigungen für Bucket eines Buckets ermöglichen, dass einzelne Objekte öffentlich gemacht werden (schreibgeschützt). Sie können eine der folgenden Optionen wählen, wenn Sie Zugriffsberechtigungen für ein einzelnes Objekt konfigurieren:

- Privat— Das Objekt ist nur von Ihnen oder jedem, auf den Sie Zugriff gewähren, lesbar.
- Öffentlich (schreibgeschützt)— Das Objekt ist für jedermann im Internet lesbar. Das einzelne Objekt wird von jedermann im Internet über die URL des Buckets lesbar (z. B.`https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`) enthalten.

Weitere Informationen zu den Zugriffsberechtigungen für einzelne Objekte finden Sie unter Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket.

Kontenübergreifender Zugriff

Verwenden Sie den kontoübergreifenden Zugriff, um anderen AWS-Konten und deren Benutzern authentifizierten Nur-Lese-Zugriff auf alle Objekte in einem Bucket zu gewähren. Der kontoübergreifende Zugriff ist ideal, wenn Sie Objekte mit einem anderen AWS-Konto teilen möchten. Wenn Sie kontoübergreifenden Zugriff auf ein anderes AWS-Konto gewähren, haben Benutzer in diesem Konto über die URL des Buckets schreibgeschützten Zugriff auf Objekte in einem Bucket (z. B. `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`). Sie können Zugriff auf maximal 10 AWS-Konten gewähren.

Weitere Informationen zum Konfigurieren des kontoübergreifenden Zugriffs finden Sie unterKonfigurieren des kontoübergreifenden Zugriffs für einen Bucket.

Access keys (Zugriffsschlüssel)

Verwenden Sie Zugriffsschlüssel, um eine Gruppe von Anmeldeinformationen zu erstellen, die vollständigen Lese- und Schreibzugriff auf einen Bucket und seine Objekte gewähren. Access keys (Zugriffsschlüssel) bestehen sowie aus einer Access keys (Zugriffsschlüssel)-ID als auch aus einem geheimen Zugriffsschlüssel. Sie können maximal zwei Zugriffsschlüssel pro Bucket besitzen. Sie können Zugriffsschlüssel für Ihre Anwendung so konfigurieren, dass sie auf Ihren Bucket und seine

Objekte mit den AWS-APIs und AWS-SDKs zugreifen können. Sie können Zugriffsschlüssel auch mit der AWS-CLI konfigurieren.

Weitere Informationen zum Erstellen von Zugriffsschlüsseln finden Sie unter Erstellen von Zugriffsschlüsseln für einen Bucket.

Resource access (Ressourcenzugriff)

Verwenden Sie den Zugriff auf Ressourcen, um einem Bucket und seinen Objekten für Lightsail-Instances vollständigen Lese- und Schreibzugriff zu gewähren. Mit dem Zugriff auf Ressourcen müssen Sie keine Anmeldeinformationen wie Zugriffsschlüssel verwalten. Um Zugriff auf eine Instance zu gewähren, fügen Sie die Instance einem Bucket in derselben AWS-Region hinzu. Sie können den Zugriff verweigern, indem Sie die Instance vom Bucket trennen. Resource access (Ressourcenzugriff) ist ideal, wenn Sie eine Anwendung auf Ihrer Instance konfigurieren, um Dateien in Ihrem Bucket programmgesteuert hochzuladen und darauf zuzugreifen. Ein solcher Anwendungsfall besteht darin, eine WordPress-Instance so zu konfigurieren, dass Mediendateien in einem Bucket gespeichert werden. Weitere Informationen finden Sie unter Tutorial: Verbinden Ihrer WordPress-Instance mit einem Bucket und Tutorial: Verwenden eines Buckets mit einer Netzwerkverteilung für die Bereitstellung von Inhalten.

Weitere Informationen zum Konfigurieren des Zugriffs auf Ressourcen finden Sie unter Konfigurieren des Zugriff auf Ressourcen für einen Bucket.

Amazon S3 Block Public Access

Benutzen Sie das Feature Amazon S3 Block Public Access, um den öffentlichen Zugriff auf Buckets in Amazon S3 und in Lightsail zentral zu beschränken. Block Public Access kann alle Amazon-S3- und Lightsail-Buckets privat machen, unabhängig von den einzelnen Bucket- und Objektberechtigungen, die möglicherweise konfiguriert wurden. Sie können die Amazon S3 Konsole, AWS-CLI, AWS-SDKs und REST-API verwenden, um die Einstellungen für Blockieren des öffentlichen Zugriffs für alle Buckets in Ihrem Konto zu konfigurieren, einschließlich der Buckets im Lightsail-Objektspeicherservice. Weitere Informationen finden Sie unter Blockieren des öffentlichen Zugriffs für Buckets.

Hochladen von Dateien in einen Amazon Lightsail-Bucket

Wenn Sie eine Datei in Ihren Bucket im Amazon Lightsail-Objektspeicherdienst hochladen, wird sie als Objekt gespeichert. Objekte umfassen die Datei und die Metadaten, die das Objekt beschreiben. Sie können in einem Bucket beliebig viele Objekte speichern.

Sie können beliebige Dateitypen – Bilder, Backups, Daten, Filme usw. – in einen Bucket hochladen. Die maximale Dateigröße, die Sie über die Lightsail-Konsole hochladen können, beträgt 2 GB. Um eine größere Datei hochzuladen, verwenden Sie die Lightsail-API, AWS Command Line Interface (AWS CLI) oder AWS SDKs.

Lightsail bietet je nach Größe der Datei, die Sie hochladen möchten, die folgenden Optionen:

- Hochladen eines Objekts mit einer Größe von bis zu 2 GB mithilfe der Lightsail-Konsole – Mit der Lightsail-Konsole können Sie ein einzelnes Objekt mit einer Größe von bis zu 2 GB hochladen. Weitere Informationen finden Sie unter Hochladen von Dateien in einen Bucket mithilfe der Lightsail-Konsole weiter unten in diesem Leitfaden.
- Hochladen eines Objekts mit bis zu 5 GB Größe in einem einzigen Vorgang mithilfe von AWS-SDKs, der REST-API oder der AWS CLI – Mit einem einzigen PUT-Vorgang können Sie ein einzelnes Objekt mit einer Größe von bis zu 5 GB hochladen. Weitere Informationen finden Sie unter Hochladen von Dateien in einen Bucket mithilfe des AWS CLI weiter unten in diesem Leitfaden.
- Hochladen eines Objekts in Teilen über die AWS-SDKs, die REST-API oder AWS CLI – Über die API für mehrteilige Uploads können Sie ein einzelnes großes Objekt mit einer Größe von 5 MB bis zu 5 TB hochladen. Die API für mehrteilige Uploads ist darauf ausgelegt, die Upload-Leistung für größere Objekte zu verbessern. Sie können ein Objekt in Teilen hochladen. Diese Objektteile können unabhängig, in jeder beliebigen Reihenfolge und parallel hochgeladen werden. Weitere Informationen finden Sie unter Hochladen von Dateien in einen Bucket mithilfe von mehrteiligen Uploads.

Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Objektschlüsselnamen und Versioning

Wenn Sie eine Datei mit der Lightsail-Konsole hochladen, wird der Dateiname als Objektschlüsselname verwendet. Der Objektschlüssel (oder Schlüsselname) identifiziert das Objekt in einem Bucket eindeutig. Der Ordner, in den die Datei hochgeladen wird, wird als Schlüsselnamen-Präfix verwendet. Wenn Sie zum Beispiel eine Datei mit Namen `sailbot.jpg` in einen Ordner in Ihrem Bucket namens `images` hochladen, wird der vollständige Objektschlüsselname und das Präfix `images/sailbot.jpg`. Allerdings wird das Objekt in der Konsole als `sailbot.jpg` im Ordner `images` angezeigt. Weitere Informationen über Objektspeichernamen finden Sie unter Schlüsselnamen für Objektspeicher-Buckets.

Wenn Sie ein Verzeichnis mit der Lightsail-Konsole hochladen, werden alle Dateien und Unterordner im Verzeichnis in den Bucket hochgeladen. Lightsail weist dann einen Objektschlüsselnamen zu, der eine Kombination aus jedem der hochgeladenen Dateinamen und dem Ordnernamen ist. Wenn Sie beispielsweise einen Ordner mit dem Namen hochladen, `images` der zwei Dateien, `sample1.jpg` und , enthält`sample2.jpg`, lädt Lightsail die Dateien hoch und weist dann die entsprechenden Schlüsselnamen `images/sample1.jpg` und zu`images/sample2.jpg`. Die Objekte werden in der -Konsole als`sample1.jpg`und`sample2.jpg`im`images`folder.

Wenn Sie eine Datei mit einem bereits vorhandenen Schlüsselnamen hochladen, und Ihr Buckethat keine Versioning aktiviert, ersetzt das neu hochgeladene Objekt das vorherige Objekt. Wenn für Ihren Bucket jedoch das Versioning aktiviert ist, erstellt Lightsail eine neue Version des Objekts, anstatt das vorhandene Objekt zu ersetzen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen der Bucket-Objekt-Versionsverwaltung.

Hochladen von Dateien in einen Bucket mithilfe der Lightsail-Konsole

Führen Sie das folgende Verfahren aus, um Dateien und Verzeichnisse mit der Lightsail-Konsole hochzuladen.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Speicher aus.
3. Wählen Sie in der Liste Buckets den Namen des Buckets aus, in den Ihre Ordner oder Dateien hochgeladen werden sollen.
4. In derObjekteFühren Sie eine der folgenden Aktionen durch:

   - Ziehen Sie Dateien und Ordner in den OrdnerObjekteangezeigten.
   - Klicken Sie aufHochladen, und wählen SieDatei, um eine einzelne Datei hochzuladen, oderDirectory, um einen Ordner und seinen gesamten Inhalt hochzuladen.

   > **Note**
   >
   > Sie können einen Ordner auch in erstellen, indem Sie Erstellen eines neuen Ordners auswählen. Sie können dann in den neuen Ordner navigieren und Dateien in diesen hochladen.

   Eine Upload erfolgreich-Meldung wird angezeigt, wenn der Upload abgeschlossen ist.

Hochladen von Dateien in einen Bucket mithilfe der AWS CLI

Vervollständigen Sie das folgende Verfahren, um Objekte in einen Bucket mithilfe der AWS Command Line Interface (AWS CLI) hochzuladen. Führen Sie dazu den Befehl `put-object` aus. Weitere Informationen finden Sie unter put-object in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die installieren AWS CLI und für Lightsail und Amazon S3 konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Verwenden Sie den folgenden Befehl in Ihrem Terminal, um Ihre Eingabedatei in Ihren -Bucket hochzuladen.

   ```
   aws s3api put-object --bucket BucketName --key ObjectKey --body LocalDirectory --
   acl bucket-owner-full-control
   ```

   Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

   - *`BucketName`* durch den Namen des Buckets, in den Sie die Datei hochladen möchten.
   - *`ObjectKey`* mit dem vollständigen Objektschlüssel des Objekts in Ihrem Bucket.
   - *`LocalDirectoryFire`* durch den lokalen Verzeichnisordnerpfad auf Ihrem Computer der hochzuladenden Datei.

   Beispiel:

   - Auf einem Linux- oder Unix-Computer:

     ```
     aws s3api put-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg --
     body home/user/Pictures/sailbot.jpg --acl bucket-owner-full-control
     ```

   - Auf einem Windows-Computer:

     ```
     aws s3api put-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg --
     body "C:\Users\user\Pictures\sailbot.jpg" --acl bucket-owner-full-control
     ```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

```
C:\>aws s3api put-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg --body "C:\Users\user\Pictures\sailbot.jpg"
{
    "ETag": "\"694d34edexampled92d64f342aa234c3\""
}
```

Konfigurieren der AWS CLI für IPv6-onlyAnforderungen

Amazon S3 unterstützt den Bucket-Zugriff über IPv6. Sie stellen Anforderungen Amazon-S3-API-Aufrufen über IPv6, indem Sie Dual-Stack-Endpunkte verwenden. Dieser Abschnitt enthält Beispiele dafür, wie Anforderungen über IPv6 an einen Dual-Stack-Endpunkt gestellt werden. Weitere Informationen finden Sie unter Verwenden von Amazon S3-Dual-Stack-Endpunkten im Amazon S3-Benutzerhandbuch. Anweisungen zum Einrichten der finden Sie AWS CLIunter Konfigurieren der AWS Command Line Interface für die Arbeit mit Amazon Lightsail.

> **Important**
>
> Der Client und das Netzwerk, die auf den Bucket zugreifen, müssen für IPv6 aktiviert sein. Weitere Informationen finden Sie unter IPv6-Erreichbarkeit.

Es gibt zwei Möglichkeiten, S3-Anforderungen von einer IPv6-onlyInstance aus zu stellen. Sie können so konfigurierenAWS CLI, dass alle Amazon S3-Anforderungen an den Dual-Stack-Endpunkt für das angegebene weitergeleitet werdenAWS-Region. Oder wenn Sie einen Dual-Stack-Endpunkt nur für bestimmte AWS CLI Befehle (nicht für alle Befehle) verwenden möchten, können Sie den S3-Dual-Stack-Endpunkt jedem Befehl hinzufügen.

Konfigurieren des AWS CLI

Legen Sie den Konfigurationswert `true` in einem Profil in Ihrer AWS Config-Datei `use_dualstack_endpoint` auf fest, um alle Amazon S3-Anforderungen, die von den Amazon S3- und s3api-AWS CLIBefehlen gestellt werden, an den Dual-Stack-Endpunkt für die angegebene Region weiterzuleiten. Sie geben die Region in der AWS CLI Konfigurationsdatei oder in einem Befehl mit der Option --region an.

Geben Sie die folgenden Befehle ein, um die zu konfigurierenAWS CLI.

```
aws configure set default.s3.use_dualstack_endpoint true
```

```
aws configure set default.s3.addressing_style virtual
```

Hinzufügen des Dual-Stack-Endpunkts zu einem bestimmten Befehl

Sie können den Dual-Stack-Endpunkt pro Befehl verwenden, indem Sie den `--endpoint-url` Parameter auf `https://s3.dualstack.`*`aws-region`*`.amazonaws.com` oder `http://s3.dualstack.`*`aws-region`*`.amazonaws.com` für jeden s3- oder s3api-Befehl setzen. Ersetzen Sie im folgenden Beispiel *`bucketname`* und *`aws-region`* durch den Namen Ihres Buckets und Ihres AWS-Region.

```
aws s3api list-objects --bucket bucketname --endpoint-url https://s3.dualstack.aws-region.amazonaws.com
```

Verwalten von Buckets und Objekten in Lightsail

Dies sind die allgemeinen Schritte zur Verwaltung Ihres Lightsail-Objektspeicher-Buckets:

1. Erfahren Sie mehr über Objekte und Buckets im Amazon Lightsail-Objektspeicherdienst. Weitere Informationen finden Sie unter Objektspeicher in Amazon Lightsail.
2. Erfahren Sie mehr über die Namen, die Sie Ihren Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Regeln für die Bucket-Benennung in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherdienst, indem Sie einen Bucket erstellen. Weitere Informationen finden Sie unter Erstellen von Buckets in Amazon Lightsail.
4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren. Weitere Informationen finden Sie unter Bewährte Methoden für die Sicherheit von Amazon Lightsail-Objektspeichern und Grundlegendes zu Bucket-Berechtigungen in Amazon Lightsail.

   Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

   - Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail

- Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail
- Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
- Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
- Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail
- Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail

5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherdienst
   - Zugriffsprotokollformat für einen Bucket im Amazon Lightsail-Objektspeicherdienst
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicherdienst
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail zum Identifizieren von Anforderungen
6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gibt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets in Amazon Lightsail .
7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unter Grundlegendes zu Objektschlüsselnamen in Amazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Hochladen von Dateien in einen Bucket in Amazon Lightsail
   - Hochladen von Dateien in einen Bucket in Amazon Lightsail mit mehrteiligem Upload
   - Anzeigen von Objekten in einem Bucket in Amazon Lightsail
   - Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
   - Herunterladen von Objekten aus einem Bucket in Amazon Lightsail
   - Filtern von Objekten in einem Bucket in Amazon Lightsail
   - Markieren von Objekten in einem Bucket in Amazon Lightsail
   - Löschen von Objekten in einem Bucket in Amazon Lightsail
9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.

10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.
11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.
12. Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen in Amazon Lightsail.
13. Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Plans Ihres Buckets in Amazon Lightsail.
14. Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.
    - Tutorial: Verbinden einer WordPress Instance mit einem Amazon Lightsail-Bucket
    - Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Netzwerkverteilung für die Bereitstellung von Inhalten in Lightsail
15. Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

Container-Services in Amazon Lightsail

Importieren in Amazon Lightsail-Container-Services ist eine hochgradig skalierbare Rechen- und Netzwerkressource, auf der Sie Container bereitstellen, ausführen und verwalten können. Ein Container ist eine Standardeinheit von Software, die Code und seine Abhängigkeiten zusammen packt, sodass die Anwendung schnell und zuverlässig von einer Computerumgebung zur anderen ausgeführt wird.

Sie können sich Ihre Lightsail-Container-Service als Computerumgebung vorstellen, mit der Sie Container in der AWS-Infrastruktur verwenden, indem Sie Images verwenden, die Sie auf Ihrem lokalen Computer erstellen und an Ihren Service senden, oder Images aus einem Online-Repository wie Amazon ECR Public Gallery.

Sie können Container auch lokal auf Ihrem lokalen Computer ausführen, indem Sie Software wie Docker installieren. Amazon Elastic Container Service (Amazon ECS) und Amazon Elastic Compute Cloud (Amazon EC2) sind andere Ressourcen innerhalb der AWS-Infrastruktur, auf denen Sie Container ausführen können. Weitere Informationen finden Sie im Amazon ECS-Entwicklerhandbuch.

Inhalt

Container

Ein Container ist eine Standardeinheit von Software, die Code und seine Abhängigkeiten zusammen packt, sodass die Anwendung schnell und zuverlässig von einer Computerumgebung zur anderen ausgeführt wird. Sie können einen Container in Ihrer Entwicklungsumgebung ausführen, ihn in Ihrer Vorproduktionsumgebung bereitstellen und dann in Ihrer Produktionsumgebung bereitstellen. Ihre Container werden zuverlässig ausgeführt, unabhängig davon, ob Ihre Entwicklungsumgebung Ihr lokaler Computer ist, Ihre Vorproduktionsumgebung ein physischer Server in einem Rechenzentrum ist oder ob Ihre Produktionsumgebung ein virtueller privater Server in der Cloud ist.

Ein Container-Image ist ein einfaches, eigenständiges, ausführbares Softwarepaket, das alle für die Ausführung benötigten Elemente umfasst: Code, Laufzeit, Systemtools, Systembibliotheken und Einstellungen. Container-Images werden zur Laufzeit zu Containern. Durch die Containerisierung der Anwendung und ihrer Abhängigkeiten müssen Sie sich nicht mehr darüber Gedanken machen, ob Ihre Software auf dem Betriebssystem und der Infrastruktur, auf dem Sie sie bereitstellen, ordnungsgemäß ausgeführt wird. Sie können sich mehr auf den Code konzentrieren.

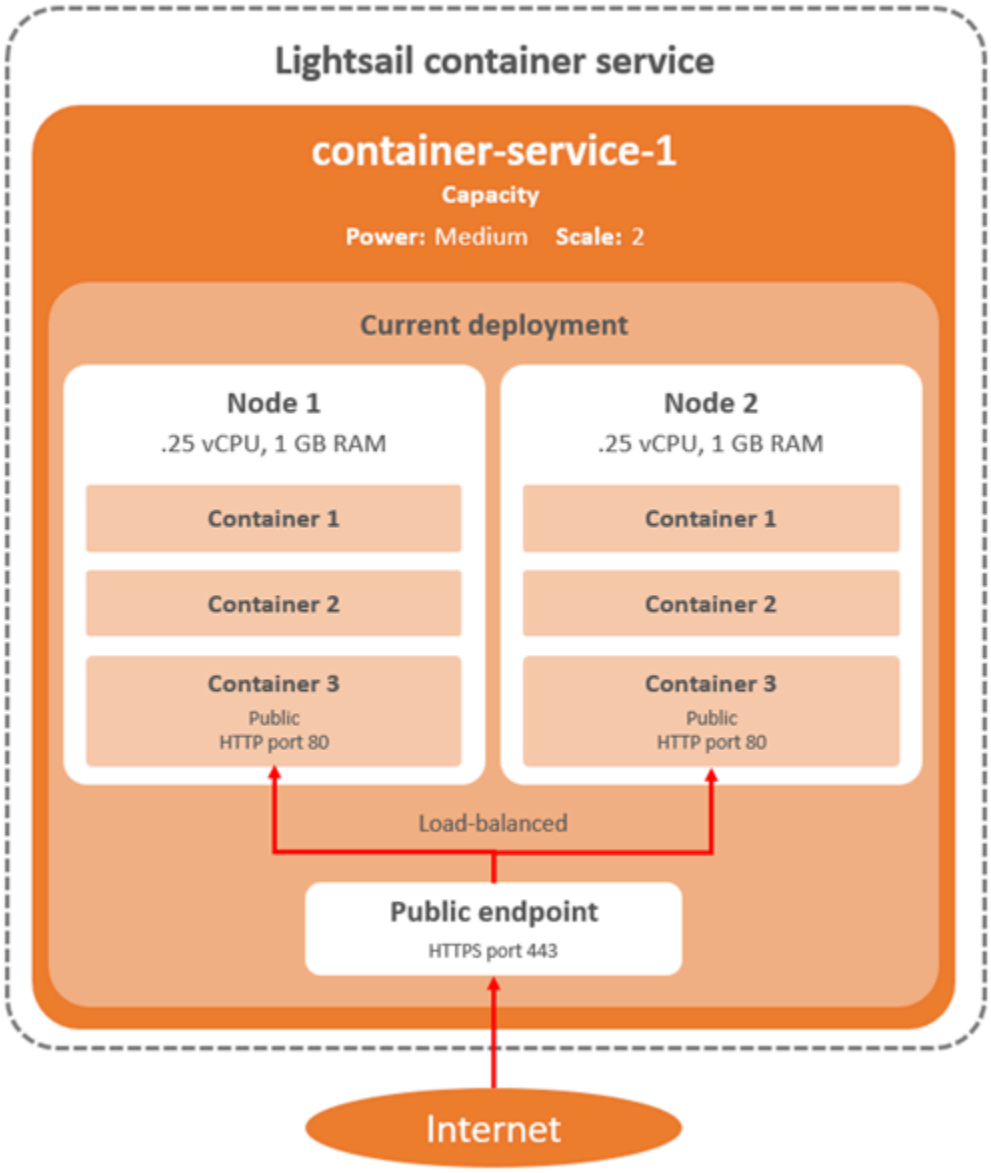
Weitere Informationen zu Containern und Container-Images finden Sie unterWas ist ein Container?imDocker-Dokumentationaus.

Elemente des Lightsail-Container-Service

Im Folgenden finden Sie die wichtigsten Elemente der Lightsail-Container-Services, die Sie vor den ersten Schritten verstehen sollten.

Lightsail-Container-Services

Ein Container-Service ist die Lightsail-Datenverarbeitungsressource, die Sie in jeder AWS-Region erstellen können, in der Lightsail verfügbar ist. Sie können Container-Services jederzeit anlegen und löschen. Weitere Informationen finden Sie unter Erstellen von Lightsail-Container-Services und Löschen von Lightsail-Container-Services.



Container-Services-Kapazität (Skalierung und Leistung)

Beim ersten Erstellen des Container-Services müssen Sie die folgenden Kapazitätsparameter auswählen:

- Skalieren - Die Anzahl der Rechenknoten, in denen Ihre Container-Workload ausgeführt werden soll. Ihre Container-Workload wird auf die Rechenknoten Ihres Dienstes kopiert. Sie können bis zu 20 Rechenknoten für einen Container-Service angeben. Sie wählen die Skalierung basierend auf der Anzahl der Knoten aus, die Ihren Dienst betreiben soll, und die für eine bessere Verfügbarkeit und höhere Kapazität erforderlich ist. Der Datenverkehr zu Ihren Containern wird über alle Knoten hinweg belastet.

- Power – Der Speicher und die vCPUs jedes Knotens in Ihrem Container-Service. Die Möglichkeiten, die Sie wählen können, sind Nano (Na), Micro (Mi), Small (Sm), Medium (Md), Large (Lg) und Xlarge (Xl), jeweils mit einer zunehmend größeren Menge an Speicher und vCPUs.

Wenn Sie den Maßstab Ihres Container-Services als mehr als 1 angeben, wird Ihre Container-Workload auf die mehreren Rechenknoten Ihres Service kopiert. Wenn der Maßstab Ihres Dienstes beispielsweise 3 ist und die Leistung Nano ist, werden drei Kopien Ihrer Container-Workload auf drei Rechenressourcen mit jeweils 512 MB RAM und 0,25 vCPUs ausgeführt. Der eingehende Datenverkehr wird zwischen den drei Ressourcen belastet. Je größer die Kapazität ist, die Sie für Ihren Container-Service auswählen, desto mehr Datenverkehr kann er verarbeiten.

Wenn Sie die Vorgehensweise in diesem Leitfaden befolgen, können Sie die Leistung und Skalierung Ihres Container-Services jederzeit dynamisch und ohne Ausfallzeiten erhöhen, wenn Sie feststellen, dass er unterprovisioniert ist, oder verringern, wenn Sie feststellen, dass er überprovisioniert ist. Lightsail verwaltet die Kapazitätsänderung automatisch zusammen mit Ihrer aktuellen Bereitstellung. Weitere Informationen finden Sie unter Ändern der Kapazität Ihrer Container-Services.

Preisgestaltung

Der monatliche Preis Ihres Container-Services wird berechnet, indem der Preis seiner Leistung mit der Anzahl seiner Rechenknoten (die Skala Ihres Service) multipliziert wird. Zum Beispiel, ein Service mit der mittleren Leistung von 40,00 USD und einer Skala von 3,00 USD kostet 120,00 pro Monat. Ihr Container-Service wird Ihnen in Rechnung gestellt, unabhängig davon, ob er aktiviert oder deaktiviert ist und ob er über eine Bereitstellung verfügt oder nicht. Sie müssen Ihren Container-Service löschen, damit er nicht mehr berechnet wird.

Jeder Container-Service umfasst unabhängig von seiner konfigurierten Kapazität ein monatliches Datenübertragungskontingent von 500 GB. Das Datenübertragungskontingent ändert sich nicht, unabhängig von der Leistung und Skalierung, die Sie für Ihren Dienst auswählen. Die Datenübertragung ins Internet, die über das Kontingent hinausgeht, führt zu einer Überschussgebühr, die je nach AWS-Region variiert und bei 0,09 USD pro GB beginnt. Die Datenübertragung aus dem Internet, die über das Kontingent hinausgeht, führt zu keiner Überschussgebühr. Weitere Informationen finden Sie in der LightsailPreisliste.

Bereitstellungen

Sie können eine Bereitstellung in Ihrem Lightsail-Container-Service. Bei einer Bereitstellung handelt es sich um eine Reihe von Spezifikationen für die Container-Workload, die Sie für Ihren Dienst starten möchten.

Sie können für jeden Container-Eintrag in einer Bereitstellung die folgenden Parameter angeben:

- Der Name Ihres Containers, der gestartet werden soll
- Das für Ihren Container zu verwendende Quell-Container-Image
- Der Befehl, der beim Starten des Containers ausgeführt wird
- Die Umgebungsvariablen, die an einen Container übergeben werden
- Die Netzwerkports, die auf Ihrem Container geöffnet werden sollen
- Der Container in der Bereitstellung, der über die Standarddomäne des Container-Services öffentlich zugänglich gemacht wird

> **Note**
>
> Nur ein Container in einer Bereitstellung kann für jeden Container-Service öffentlich zugänglich gemacht werden.

Die folgenden Integritätsprüfungsparameter gelten für den öffentlichen Endpunkt einer Bereitstellung nach dem Start:

- Der Verzeichnispfad, für den eine Integritätsprüfung durchgeführt wird.
- Erweiterte Einstellungen für die Integritätsprüfung wie Intervallsekunden, Timeout-Sekunden, Erfolgscodes, gesunder Schwellenwert und ungesunder Schwellenwert.

Ihr Container-Service kann jeweils eine aktive Bereitstellung haben, und eine Bereitstellung kann bis zu 10 Containereinträge enthalten. Sie können eine Bereitstellung gleichzeitig erstellen, wenn Sie den Container Service erstellen, oder Sie können ihn erstellen, nachdem der Dienst ausgeführt wird. Weitere Informationen finden Sie unter Erstellen und Verwalten von Bereitstellungen für Container-Services.

Bereitstellungs-Versionen

Jede Bereitstellung, die Sie in Ihrem Amazon Lightsail-Container-Service erstellen, wird als Bereitstellungsversion gespeichert. Wenn Sie die Parameter einer vorhandenen Bereitstellung ändern, werden die Container erneut für Ihren Dienst bereitgestellt, und die geänderte Bereitstellung führt zu einer neuen Bereitstellungsversion. Die neuesten 50 Bereitstellungsversionen für jeden Container-Service werden gespeichert. Sie können jede der 50 Bereitstellungsversionen verwenden, um eine neue Bereitstellung im selben Container-Service zu erstellen. Weitere Informationen finden Sie unter Erstellen und Verwalten von Bereitstellungen für Container-Services.

Container-Image-Quellen

Wenn Sie eine Bereitstellung erstellen, müssen Sie für jeden Containereintrag in der Bereitstellung ein Quellcontainer-Image angeben. Unmittelbar nach dem Erstellen der Bereitstellung ruft der Container-Service die Images aus den angegebenen Quellen ab und verwendet sie zum Erstellen der Container.

Die angegebenen Bilder können von den folgenden Quellen stammen:

- Ein öffentliches Register, wie beispielsweise Amazon ECR Public Gallery, oder ein anderes öffentliches Container-Image-Register. Weitere Informationen zu Amazon ECR Public finden Sie unter Was ist Amazon Elastic Container Registry Public? im Benutzerhandbuch von Amazon ECR.
- Push-Images von Ihrem lokalen Rechner an Ihren Container-Service. Wenn Sie Container-Images auf Ihrem lokalen Computer erstellen, können Sie sie an Ihren Container-Service senden, um sie beim Erstellen einer Bereitstellung zu verwenden. Weitere Informationen finden Sie unter Container-Service-Images erstellen und Container-Images übertragen und verwalten.

Lightsail-Container-Images unterstützen Linux-basierte Container-Images. Windows-basierte Container-Images werden derzeit nicht unterstützt, sie können jedoch Docker, die AWS Command Line Interface (AWS CLI) und das Lightsail-Control-(lightsailctl)-Plugin unter Windows ausführen, um Ihre Linux-basierten Images auf Ihre Lightsail-Container-Service zu übertragen.

Öffentliche Endpunkte und Standarddomänen

Wenn Sie eine Bereitstellung erstellen, können Sie den Containereintrag in der Bereitstellung angeben, der als öffentlicher Endpunkt Ihres Container-Services dient. Die Anwendung auf dem öffentlichen Endpunktcontainer ist im Internet über eine zufällig generierte

Standarddomäne Ihres Container-Services öffentlich zugänglich. Die Standard-Domain ist als `https://<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`, in dem *`<ServiceName>`* der Name Ihres Container-Services ist. *`<RandomGUID>`* ist eine zufällig generierte globale eindeutige Kennung Ihres Container-Services in der AWS-Region für Ihr Lightsail-Konto und *`<AWSRegion>`* ist die AWS-Region, in der der Container-Service erstellt wurde. Der öffentliche Endpunkt von Lightsail-Container-Services unterstützt nur HTTPS und unterstützt keinen TCP- oder UDP-Datenverkehr. Nur ein Container kann der öffentliche Endpunkt für einen Dienst sein. Stellen Sie also sicher, dass Sie den Container, der das Front-End Ihrer Anwendung hostet, als öffentlichen Endpunkt auswählen, während auf die restlichen Container intern zugegriffen werden kann.

Sie können die Standarddomäne Ihres Container-Dienstes verwenden, oder Sie können Ihre eigene Domäne verwenden (Ihren registrierten Domänennamen). Weitere Informationen zur Verwendung von benutzerdefinierten Domains mit Ihren Container-Services finden Sie unter Aktivieren und Verwalten benutzerdefinierter Domains für Ihre Container-Services.

Private Domain

Alle Container-Services verfügen auch über eine private Domäne mit einer *`<ServiceName>`*`.service.local`-Formatierung, in dem der Name Ihres Container-Servicess *`<ServiceName>`* lautet. Verwenden Sie die private Domain, um von einer anderen Ihrer Lightsail-Ressourcen in derselben AWS-Region wie Ihr Service auf Ihren Container-Service zuzugreifen. Die private Domäne ist die einzige Möglichkeit, auf Ihren Container-Service zuzugreifen, wenn Sie in der Bereitstellung Ihres Dienstes keinen öffentlichen Endpunkt angeben. Eine Standarddomäne wird für Ihren Container-Service generiert, auch wenn Sie keinen öffentlichen Endpunkt angeben, aber es wird eine `404 No Such Service`-Fehlermeldung anzeigen, wenn Sie versuchen, zu ihm zu navigieren.

Um mit der privaten Domäne Ihres Container-Services auf einen bestimmten Container zuzugreifen, müssen Sie den offenen Port des Containers angeben, der Ihre Verbindungsanforderung akzeptiert. Sie tun dies, indem Sie die Domain Ihrer Anfrage als *`<ServiceName>`*`.service.local:`*`<PortNumber>`*, in dem *`<ServiceName>`*. Dies ist der Name Ihres Container-Dienstes und *`<PortNumber>`* ist der offene Port des Containers, mit dem Sie eine Verbindung herstellen möchten. Wenn Sie beispielsweise eine Bereitstellung für Ihren Container-Service mit dem Name`container-service-1`, und Sie geben einen Redis-Container mit Port `6379` öffnen, sollten Sie die Domain Ihrer Anfrage als *`container-service-1`*`.service.local:`*`6379`* aus.

Benutzerdefinierte Domänen und SSL-/TLS-Zertifikate

Sie können bis zu 4 Ihrer benutzerdefinierten Domänen mit Ihrem Container-Service verwenden, anstatt die Standarddomäne zu verwenden. Zum Beispiel können Sie den Datenverkehr für Ihre benutzerdefinierte Domäne leiten, wie etwa `example.com` an den Container in der Bereitstellung, der als öffentlicher Endpunkt gekennzeichnet ist.

Um Ihre benutzerdefinierten Domänen mit Ihrem Dienst zu verwenden, müssen Sie zunächst ein SSL/TLS-Zertifikat für die Domänen anfordern, die Sie verwenden möchten. Validieren Sie das SSL-/TLS-Zertifikat, indem Sie einen CNAME-Aktensatz zum DNS Ihrer Domänen hinzufügen. Nachdem das SSL-/TLS-Zertifikat validiert wurde, aktivieren Sie benutzerdefinierte Domänen auf Ihrem Container-Service, indem Sie das gültige SSL-/TLS-Zertifikat an Ihren Dienst anhängen. Weitere Informationen finden Sie unter Erstellen von SSL-/TLS-Zertifikaten für Ihre Lightsail-Container-Services, Validierung von SSL-/TLS-Zertifikaten für Ihre Lightsail-Container-Services, und Aktivieren und Verwalten benutzerdefinierter Domains für Ihre Lightsail-Container-Services.

Containerprotokolle

Jeder Container in Ihrem Container-Service generiert ein Protokoll, auf das Sie zugreifen können, um den Betrieb Ihrer Container zu diagnostizieren. Die Protokolle stellen die stdout- und stderr-Streams von Prozessen, die innerhalb des Containers ausgeführt werden. Weitere Informationen finden Sie unter Anzeigen von Container-Services-Protokollen.

Metriken

Überwachen Sie die Metriken Ihres Container-Services, um Probleme zu diagnostizieren, die aufgrund einer übermäßigen Auslastung auftreten können. Sie können auch Metriken überwachen, um festzustellen, ob Ihr Service nicht bereitgestellt oder überbereitgestellt ist. Weitere Informationen finden Sie unter Anzeigen von Container-Services-Metriken.

Verwendung von Lightsail-Container-Services

Dies sind die allgemeinen Schritte für die Verwaltung Ihres Lightsail-Container-Service, wenn Sie vorhaben, Container-Images von Ihrem lokalen Computer an Ihren Dienst zu übertragen und in Ihrer Bereitstellung zu verwenden:

1. Erstellen Sie Ihren Container-Service in Ihrem Lightsail-Konto. Weitere Informationen finden Sie unter Erstellen von Lightsail-Container-Services.

2. Erfahren Sie mehr über die Software, die Sie benötigen, um Ihre eigenen Container-Images auf Ihrem lokalen Computer zu erstellen, und Sie sie dann auf Ihren Lightsail-Container-Service zu schieben. Weitere Informationen finden Sie unter finden Sie in den folgenden Anleitungen:
   - Installieren von Software zum Verwalten von Container-Images für Ihre Lightsail-Container-Services
   - Erstellen von Container-Images für Ihre Lightsail-Container-Services
   - Verschieben und Verwalten von Container-Images auf Ihren Lightsail-Container-Services
3. Erstellen Sie eine Bereitstellung in Ihrem Container-Service, mit der Ihre Container konfiguriert und gestartet werden. Weitere Informationen finden Sie unter Erstellen und Verwalten von Bereitstellungen für Ihre Lightsail-Container-Services.
4. Zeigen Sie frühere Bereitstellungen für Ihren Container-Service an. Sie können eine neue Bereitstellung mit einer früheren Bereitstellungsversion erstellen. Weitere Informationen finden Sie unter Anzeigen und Verwalten von Bereitstellungsversionen Ihrer Lightsail-Container-Services.
5. Zeigen Sie die Containerprotokolle auf Ihrem Container-Services an. Weitere Informationen finden Sie unter Anzeigen der Containerprotokolle Ihrer Lightsail-Container-Services.
6. Erstellen Sie ein SSL-/TLS-Zertifikat für die Domänen, die Sie mit den Containern verwenden möchten. Weitere Informationen finden Sie unter Erstellen von SSL-/TLS-Zertifikaten für Ihre Lightsail-Container-Services.
7. Validieren Sie das SSL-/TLS-Zertifikat, indem Sie Akten zum DNS Ihrer Domänen hinzufügen. Weitere Informationen finden Sie unter Validierung von SSL-/TLS-Zertifikaten für Ihre Lightsail-Container-Services.
8. Aktivieren Sie benutzerdefinierte Domänen, indem Sie Ihrem Container-Service ein gültiges SSL-/TLS-Zertifikat anfügen. Weitere Informationen finden Sie unter Aktivieren und Verwalten benutzerdefinierter Domains für Ihre Lightsail-Container-Services.
9. Überwachen Sie die Auslastungsmetriken Ihres Container-Services. Weitere Informationen finden Sie unter Anzeigen von Container-Services-Metriken.
10. (Optional) Skalieren Sie die Kapazität Ihres Container-Services vertikal, indem Sie die Leistungsspezifikation erhöhen und horizontal, indem Sie die Skalierungsspezifikation erhöhen. Weitere Informationen finden Sie unter Ändern der Kapazität Ihrer Lightsail-Container-Services.
11. Löschen Sie Ihren Container-Service, wenn Sie ihn nicht verwenden, um monatliche Gebühren zu vermeiden. Weitere Informationen finden Sie unter Löschen von Lightsail-Container-Services.

Dies sind die allgemeinen Schritte für die Verwaltung Ihres Lightsail-Container-Services, wenn Sie Container-Images aus einer öffentlichen Registry in Ihrer Bereitstellung verwenden möchten:

1. Erstellen Sie Ihren Container-Service in Ihrem Lightsail-Konto. Weitere Informationen finden Sie unter Erstellen von Lightsail-Container-Services.
2. Wenn Sie planen, Container-Images aus einer öffentlichen Registry zu verwenden, suchen Sie Container-Images in einem öffentlichen Register wie Amazon ECR Public Gallery. Weitere Informationen zu Amazon ECR Public finden Sie unter Was ist Amazon Elastic Container Registry Public? im Benutzerhandbuch von Amazon ECR.
3. Erstellen Sie eine Bereitstellung in Ihrem Container-Service, mit der Ihre Container konfiguriert und gestartet werden. Weitere Informationen finden Sie unter Erstellen und Verwalten von Bereitstellungen für Ihre Lightsail-Container-Services.
4. Zeigen Sie frühere Bereitstellungen für Ihren Container-Service an. Sie können eine neue Bereitstellung mit einer früheren Bereitstellungsversion erstellen. Weitere Informationen finden Sie unter Anzeigen und Verwalten von Bereitstellungsversionen Ihrer Lightsail-Container-Services.
5. Zeigen Sie die Containerprotokolle auf Ihrem Container-Services an. Weitere Informationen finden Sie unter Anzeigen der Containerprotokolle Ihrer Lightsail-Container-Services.
6. Erstellen Sie ein SSL-/TLS-Zertifikat für die Domänen, die Sie mit den Containern verwenden möchten. Weitere Informationen finden Sie unter Erstellen von SSL-/TLS-Zertifikaten für Ihre Lightsail-Container-Services.
7. Validieren Sie das SSL-/TLS-Zertifikat, indem Sie Akten zum DNS Ihrer Domänen hinzufügen. Weitere Informationen finden Sie unter Validierung von SSL-/TLS-Zertifikaten für Ihre Lightsail-Container-Services.
8. Aktivieren Sie benutzerdefinierte Domänen, indem Sie Ihrem Container-Service ein gültiges SSL-/TLS-Zertifikat anfügen. Weitere Informationen finden Sie unter Aktivieren und Verwalten benutzerdefinierter Domains für Ihre Lightsail-Container-Services.
9. Überwachen Sie die Auslastungsmetriken Ihres Container-Services. Weitere Informationen finden Sie unter Anzeigen von Container-Services-Metriken.
10. (Optional) Skalieren Sie die Kapazität Ihres Container-Services vertikal, indem Sie die Leistungsspezifikation erhöhen und horizontal, indem Sie die Skalierungsspezifikation erhöhen. Weitere Informationen finden Sie unter Ändern der Kapazität Ihrer Lightsail-Container-Services.
11. Löschen Sie Ihren Container-Service, wenn Sie ihn nicht verwenden, um monatliche Gebühren zu vermeiden. Weitere Informationen finden Sie unter Löschen von Lightsail-Container-Services.

Erstellen eines Lightsail-Container-Services

In diesem Leitfaden zeigen wir Ihnen, wie Sie einen Amazon Lightsail-Container-Service, mit derLightsail-Konsole erstellen und beschreiben die Einstellungen des Container-Services, die Sie konfigurieren können.

Bevor Sie beginnen, empfehlen wir, dass Sie sich mit den Elementen eines Lightsail-Container-Services vertraut machen. Weitere Informationen finden Sie unter Container-Services.

Container-Service-Kapazität (Skalierung und Leistung)

Sie müssen die Kapazität Ihres Container-Servicess auswählen, wenn Sie ihn zum ersten Mal erstellen. Die Kapazität besteht aus einer Kombination der folgenden Parameter:

- Skalieren - Die Anzahl der Computing-Knoten, in denen Ihre Container-Workload ausgeführt werden soll. Ihre Container-Workload wird auf die Computing-Knoten Ihres Dienstes kopiert. Sie können bis zu 20 Rechenknoten für einen Container-Service angeben. Sie wählen die Skalierung basierend auf der Anzahl der Knoten aus, die Ihren Dienst betreiben soll, und die für eine bessere Verfügbarkeit und höhere Kapazität erforderlich ist. Der Datenverkehr zu Ihren Containern wird über alle Knoten hinweg belastet.
- Power - Der Speicher und die vCPUs jedes Knotens in Ihrem Container-Service. Die Möglichkeiten, die Sie wählen können, sind Nano (Na), Micro (Mi), Small (Sm), Medium (Md), Large (Lg) und Xlarge (Xl); jeweils mit einer zunehmend größeren Menge an Speicher und vCPUs.

Für den eingehenden Datenverkehr wird über die Skala (die Anzahl der Computing-Knoten) Ihres Container-Services ein Load Balancing vorgenommen. Beispielsweise werden bei einem Dienst mit einer Nano-Leistung und einer Skala von 3, 3 Kopien Ihrer Container-Workload ausgeführt. Jeder Knoten wird über 512 MB RAM und 0,25 vCPUs verfügen. Der eingehende Datenverkehr wird über die drei Knoten hinweg lastenverteilt. Je größer die Kapazität ist, die Sie für Ihren Container-Service auswählen, desto mehr Datenverkehr kann er verarbeiten.

Wenn Sie die Vorgehensweise in diesem Leitfaden befolgen, können Sie die Leistung und Skalierung Ihres Container-Services jederzeit dynamisch und ohne Ausfallzeiten erhöhen, wenn Sie feststellen, dass er unterprovisioniert ist, oder verringern, wenn Sie feststellen, dass er überprovisioniert ist. Lightsail verwaltet die Kapazitätsänderung automatisch zusammen mit Ihrer aktuellen Bereitstellung. Weitere Informationen finden Sie unter Ändern der Kapazität Ihrer Lightsail-Container-Services.

Preisgestaltung

Der monatliche Preis Ihres Container-Servicess wird berechnet, indem der Basispreis seiner Leistung mit der Skala (Anzahl der Computing-Knoten) multipliziert wird. Zum Beispiel, ein Service mit der mittleren Leistung von 40,00 USD und einer Skala von 3,00 USD kostet 120,00 pro Monat.

Jeder Container-Service umfasst unabhängig von seiner konfigurierten Kapazität ein monatliches Datenübertragungskontingent von 500 GB. Das Datenübertragungskontingent ändert sich nicht, unabhängig von der Leistung und Skalierung, die Sie für Ihren Dienst auswählen. Die Datenübertragung ins Internet, die über das Kontingent hinausgeht, führt zu einer Überschussgebühr, die je nach AWS-Region variiert und bei 0,09 USD pro GB beginnt. Die Datenübertragung aus dem Internet, die über das Kontingent hinausgeht, führt zu keiner Überschussgebühr. Weitere Informationen finden Sie in der LightsailPreisliste.

Ihr Container-Service wird Ihnen in Rechnung gestellt, unabhängig davon, ob er aktiviert oder deaktiviert ist und ob er über eine Bereitstellung verfügt oder nicht. Sie müssen Ihren Container-Service löschen, damit er nicht mehr berechnet wird. Weitere Informationen finden Sie unter Löschen von Lightsail-Container-Services.

Status des Container-Servicess

Ihr Container-Service kann in einem der folgenden Zustände sein:

- Ausstehend— Ihr Container-Service wird gerade erstellt.
- Bereit— Ihr Container-Service wird ausgeführt, hat jedoch keine aktive Containerbereitstellung.
- Bereitstellen— Ihre Bereitstellung wird in Ihrem Container-Service gestartet.
- Ausführen— Ihr Container-Service wird ausgeführt und verfügt über eine aktive Containerbereitstellung.
- Aktualisieren— Ihre Container-Servicekapazität oder ihre benutzerdefinierten Domänen werden aktualisiert.
- Löschen – Ihr Container-Service wird gelöscht. Ihr Container-Service befindet sich in diesem Zustand, nachdem Sie das Löschen ausgewählt haben, und er befindet sich nur für einen kurzen Moment in diesem Zustand.
- Deaktiviert— Ihr Container-Service ist deaktiviert, und seine aktive Bereitstellung und gegebenenfalls Container, werden heruntergefahren.

Unterstatus des Container-Servicess

Wenn sich Ihr Container-Service in einem Bereitstellen- oder Aktualisieren-Zustand befindet, wird einer der folgenden zusätzlichen Unterzustände unterhalb des Container-Servicezustands angezeigt:

- Erstellen von Systemressourcen – Die Systemressourcen für Ihren Container-Service werden erstellt.
- Erstellen einer Netzwerkinfrastruktur – Die Netzwerkinfrastruktur für Ihren Container-Service wird erstellt.
- Bereitstellungszertifikat- Das SSL-/TLS-Zertifikat für Ihren Container-Service wird erstellt.
- Bereitstellungsservice- Ihr Container-Service wird bereitgestellt.
- Erstellen einer Bereitstellung – Ihre Bereitstellung wird auf Ihrem Container-Service erstellt.
- Auswerten der Zustandsprüfung- Der Zustand Ihrer Bereitstellung wird ausgewertet.
- Aktivieren der Bereitstellung- Ihre Bereitstellung wird aktiviert.

Wenn sich Ihr Container-Service in einem Ausstehend -Zustand befindet, dann wird einer der folgenden zusätzlichen Unterzustände unterhalb des Container-Servicezustands angezeigt:

- Zertifikatslimit überschritten- Das für Ihren Container-Service erforderliche SSL-/TLS-Zertifikat überschreitet die maximal zulässige Anzahl an Zertifikaten für Ihr Konto.
- Unbekannter Fehler- Ein Fehler ist aufgetreten, als Ihr Container-Service erstellt wurde.

Erstellen eines Container-Servicess

Vervollständigen Sie den folgenden Vorgang, um Ihren Lightsail-Container-Service zu löschen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie Container-Service erstellen aus.
4. Auf der Seite Einen Container-Service erstellen, wählen Sie Ändern der AWS-Region und wählen dann eine AWS-Region für Ihren Container-Service.
5. Wählen Sie eine Kapazität für Ihren Container-Service. Weitere Informationen finden Sie im AbschnittContainer-Servicekapazität (Skalierung und Leistung)in diesem Leitfaden.
6. Vervollständigen Sie die folgenden Schritte, um eine Bereitstellung zu erstellen, die gleichzeitig mit dem Erstellen des Container-Services gestartet wird. Fahren Sie andernfalls mit Schritt 7 fort, um einen Container-Service ohne Bereitstellung zu erstellen.

Erstellen Sie einen Container-Service mit einer Bereitstellung, wenn Sie ein Container-Image aus einem öffentlichen Registry verwenden möchten. Andernfalls erstellen Sie Ihren Dienst ohne Bereitstellung, wenn Sie ein Container-Image verwenden möchten, das sich auf Ihrem lokalen Computer befindet. Sie können das Container-Image von Ihrem lokalen Computer an Ihren Container-Service senden, nachdem Ihr Dienst betriebsbereit ist. Anschließend können Sie eine Bereitstellung mithilfe des verschobenen Container-Images erstellen, das bei Ihrem Container-Service registriert ist.

a. Wählen Sie Beritstellung erstellen aus.

b. Wählen Sie eine der folgenden Optionen:

   - Wählen Sie eine Beispielbereitstellung – Wählen Sie diese Option, um eine Bereitstellung mit einem Container-Image zu erstellen, das vom Lightsail-Team mit einer Reihe von vorkonfigurierten Bereitstellungsparametern kuratiert wurde. Diese Option bietet die schnellste und einfachste Möglichkeit, einen beliebten Container für Ihren Container-Service in Betrieb zu bringen.
   - Angeben einer benutzerdefinierten Bereitstellung— Wählen Sie diese Option, um eine Bereitstellung zu erstellen, indem Sie Container Ihrer Wahl angeben.

   Die Bereitstellungsformularansicht, in der Sie neue Bereitstellungsparameter eingeben können.

c. Geben Sie die Parameter Ihrer Bereitstellung ein. Weitere Informationen zu den Bereitstellungsparametern, die Sie angeben können, finden Sie im Leitfaden Parameter für die Bereitstellung im Abschnitt Erstellen und Verwalten von Bereitstellungen für Ihre Lightsail-Container-Services.

d. Wählen SieContainereintrag hinzufügen, um Ihrer Bereitstellung mehr als einen Containereintrag hinzuzufügen. Sie können über bis zu 10 Containereinträge verfügen.

e. Wenn Sie mit der Eingabe der Parameter Ihrer Bereitstellung fertig sind, wählen SieSpeichern und Bereitstellen, um die Bereitstellung auf Ihrem Container-Service zu erstellen.

7. Geben Sie einen Namen für Ihren Container-Service ein.

   Container-Servicenamen müssen wie folgt lauten:

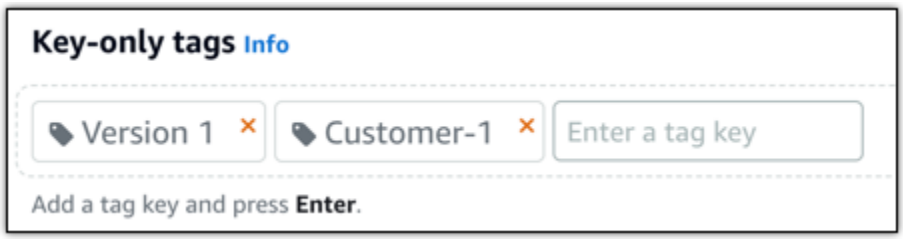
   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.

- Muss zwischen 2 und 63 Zeichen enthalten.
- Sie dürfen nur alphanumerische Zeichen und Bindestriche enthalten.
- Ein Bindestrich (-) kann Wörter trennen, kann aber nicht am Anfang oder Ende des Namens stehen.

> **Note**
>
> Der von Ihnen angegebene Name ist Teil des Standarddomänennamens Ihres Container-Servicess und wird für die Öffentlichkeit sichtbar sein.

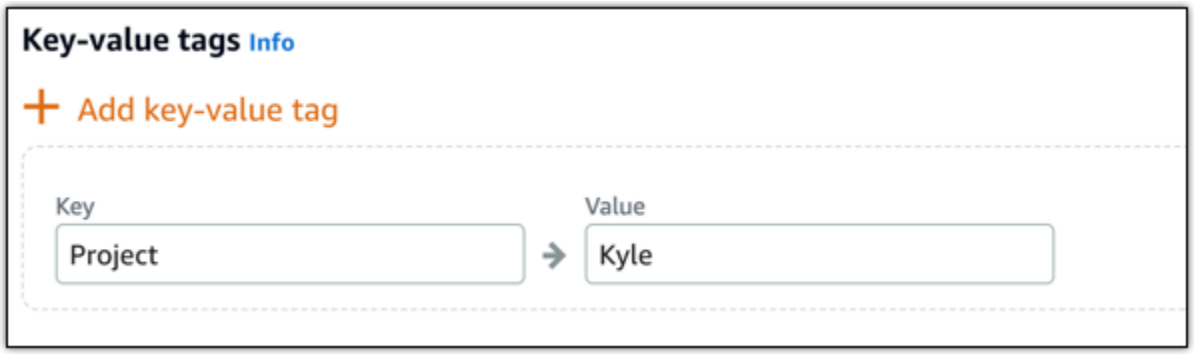
8. Wählen Sie eine der folgenden Optionen aus, um Ihrem Container-Service Tags hinzuzufügen:

- Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.



- Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

  Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.



> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

9. Wählen Sie Container-Service erstellen aus.

   Daraufhin wird die Verwaltungsseite Ihres neuen Container-Servicess angezeigt. Der Status Ihres neuen Containersdienstes lautetAusstehendwährend es erstellt wird. Nach einigen Momenten ändert sich der Status Ihres Service zuBereit, wenn es keine aktuelle Bereitstellung hat, oderAusführen, wenn Sie eine Bereitstellung erstellt haben.

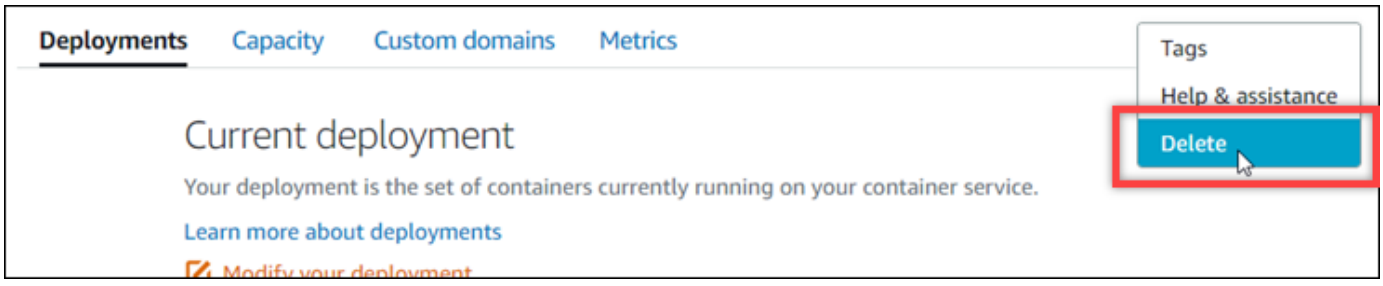
Löschen eines Lightsail-Container-Services

Sie können Ihren Amazon Lightsail-Container-Service jederzeit löschen, wenn Sie ihn nicht mehr verwenden. Wenn Sie den Container-Service löschen, werden alle Bereitstellungen und registrierten Container-Images, die diesem Dienst zugeordnet sind, dauerhaft zerstört. Die von Ihnen erstellten SSL-/TLS-Zertifikate und Domains verbleiben jedoch in Ihrem Lightsail-Konto, sodass Sie sie mit einer anderen Ressource verwenden können. Weitere Informationen zu Container-Services finden Sie unter Container-Services in Amazon Lightsail.

Löschen eines Container-Servicess

Vervollständigen Sie den folgenden Vorgang, um Ihren Container-Service zu löschen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen der Container-Servicess aus, den Sie löschen möchten.
4. Wählen Sie das Ellipsen-Symbol (⋮) im Registerkarten-Menü und wählen Sie dann Löschen aus.



5. Wählen Sie Container-Service löschen, um Ihren Dienst zu löschen.
6. Wählen Sie in der angezeigten EingabeaufforderungJa, löschen, um zu bestätigen, dass die Löschung dauerhaft ist.

   Ihr Container-Service wird nach wenigen Augenblicken gelöscht.

Lightsail-Container-Service-Images

Mit Docker können Sie verteilte, auf Containern basierende Anwendungen erstellen, ausführen, testen und bereitstellen. Amazon Lightsail-Container-Services verwenden Docker-Container-Images in Bereitstellungen, um Container zu starten.

In diesem Leitfaden zeigen wir Ihnen, wie Sie mit einer Docker-Datei ein Container-Image auf Ihrem lokalen Computer erstellen. Nachdem Ihr Image erstellt wurde, können Sie es dann an Ihren Lightsail-Container-Service senden, um es bereitzustellen.

Um die Verfahren in diesem Leitfaden durchzuführen, sollten Sie über ein grundlegendes Verständnis dessen verfügen, was ein Docker ist und wie er funktioniert. Weitere Informationen zu Docker finden Sie unter Was ist Docker? und im Thema Docker-Übersicht.

Inhalt

Schritt 1: Erfüllen der Voraussetzungen

Bevor Sie beginnen, müssen Sie die zum Erstellen von Containern erforderliche Software installieren und diese dann an Ihren Lightsail-Container-Service verschieben. Beispielsweise müssen Sie Docker installieren und verwenden, um Ihre Container-Images zu erstellen und zu entwickeln, die Sie dann mit Ihrem Lightsail-Container-Service verwenden können. Weitere Informationen finden Sie unter Installieren von Software zur Verwaltung von Container-Images für Ihre Amazon Lightsail-Container-Services.

Schritt 2: Erstellen einer Docker-Datei und Erstellen eines Container-Images

Führen Sie die folgenden Schritte aus, um eine Docker-Datei zu erstellen, und entwickeln Sie daraus ein `mystaticwebsite`-Docker-Container-Image. Das Container-Image wird für eine einfache statische Website sein, die auf einem Apache-Webserver auf Ubuntu gehostet wird.

1. Erstellen eines `mystaticwebsite`-Ordners auf Ihrem lokalen Computer, in dem Sie Ihre Docker-Datei speichern.
2. Erstellen Sie eine Docker-Datei in dem Ordner, den Sie gerade erstellt haben.

   Die Docker-Datei verwendet keine Dateierweiterung, wie `.TXT`. Der komplette Dateiname lautet `Dockerfile`.
3. Kopieren Sie einen der folgenden Codeblöcke, je nachdem, wie Sie Ihr Container-Image konfigurieren möchten und fügen Sie es in Ihre Docker-Datei ein:

   - Wenn Sie ein einfaches statisches Website-Container-Image mit einer Hello-World-Nachricht erstellen möchten, kopieren Sie den folgenden Codeblock und fügen Sie ihn in die Docker-Datei ein. In diesem Codebeispiel wird das Ubuntu-18.04-Image verwendet. Die`RUN`-Anweisungen aktualisieren die Paket-Caches, installiert und konfiguriert Apache und druckt eine Hello-World-Nachricht an das Dokumenten-Stammverzeichnis des Webservers. Die `EXPOSE`-Anweisung stellt Port 80 auf dem Container bereit, und die `CMD`-Anweisung startet den Webserver.

     ```
     FROM ubuntu:18.04

     # Install dependencies
     RUN apt-get update && \
      apt-get -y install apache2

     # Write hello world message
     RUN echo 'Hello World!' > /var/www/html/index.html

     # Open port 80
     EXPOSE 80

     # Start Apache service
     CMD ["/usr/sbin/apache2ctl", "-D", "FOREGROUND"]
     ```

- Wenn Sie Ihren eigenen Satz von HTML-Dateien für Ihr statisches Website-Container-Image verwenden möchten, erstellen Sie einen `html`-Ordner in demselben Ordner, in dem Sie Ihre Docker-Datei speichern. Legen Sie dann Ihre HTML-Dateien in diesen Ordner.

  Nachdem sich Ihre HTML-Dateien im`html`-Ordner befinden, kopieren Sie den folgenden Codeblock und fügen Sie ihn in die Docker-Datei ein. In diesem Codebeispiel wird das Ubuntu-18.04-Image verwendet. Die`RUN`-Anweisungen aktualisieren die Paket-Caches und installiert und konfiguriert Apache. Die`COPY`-Anweisung kopiert den Inhalt des HTML-Ordners in das Dokumenten-Stammverzeichnis des Webservers. Die `EXPOSE`-Anweisung stellt Port 80 auf dem Container bereit, und die `CMD`-Anweisung startet den Webserver.

  ```
  FROM ubuntu:18.04

  # Install dependencies
  RUN apt-get update && \
   apt-get -y install apache2

  # Copy html directory files
  COPY html /var/www/html/

  # Open port 80
  EXPOSE 80

  CMD ["/usr/sbin/apache2ctl", "-D", "FOREGROUND"]
  ```

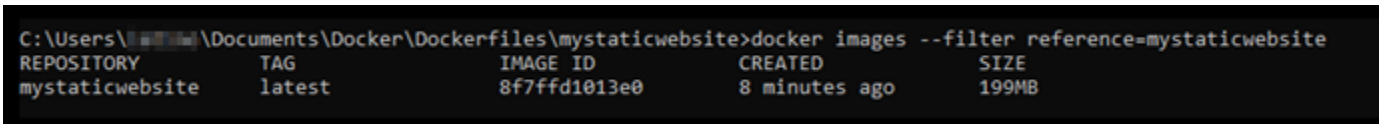
4. Öffnen Sie eine Eingabeaufforderung oder ein Terminalfenster, und ändern Sie das Verzeichnis zu dem Ordner, in dem Sie Ihre Docker-Datei speichern.
5. Geben Sie den folgenden Befehl ein, um das Container-Image mit der Docker-Datei in dem Ordner zu entwickeln. Dieser Befehl entwickelt ein neues Docker-Container-Image namens `mystaticwebsite`.

   ```
   docker build -t mystaticwebsite .
   ```

   Sie sollten eine Meldung sehen, die bestätigt, dass Ihr Image erfolgreich entwickelt wurde.
6. Geben Sie den folgenden Befehl ein, um die Container-Images auf Ihrem lokalen Computer anzuzeigen.

   ```
   docker images --filter reference=mystaticwebsite
   ```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten, das das neu erstellte Container-Image anzeigt.



Ihr neu entwickeltes Container-Image ist bereit, getestet zu werden, indem es zum Ausführen eines neuen Containers auf Ihrem lokalen Computer verwendet wird. Fahren Sie mit dem nächsten Abschnitt Schritt 3: Ausführen Ihres neuen Container-Images in diesem Leitfaden fort.

Schritt 3: Ausführen Ihres neuen Container-Images

Vervollständigen Sie die folgenden Schritte, um das neue Container-Image auszuführen, das Sie erstellt haben.

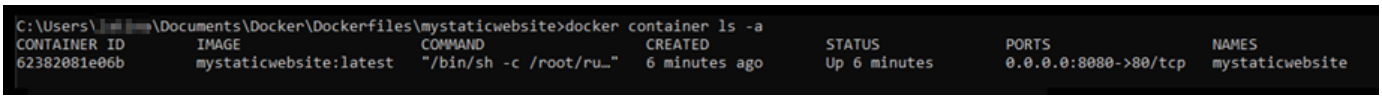
1. Geben Sie in einer Eingabeaufforderung oder einem Terminalfenster den folgenden Befehl ein, um das Container-Image auszuführen, das Sie im vorherigen Abschnitt Schritt 2: Erstellen einer Docker-Datei und Erstellen eines Containers dieses Leitfadens entwickelt haben. Die `-p 8080:80`-Option ordnet den bereitgestellten Port 80 auf dem Container, dem Port 8080 auf Ihrem lokalen Computer zu. Die `-d`-Option gibt an, dass der Container im getrennten Modus ausgeführt werden soll.

```
docker container run -d -p 8080:80 --name mystaticwebsite mystaticwebsite:latest
```

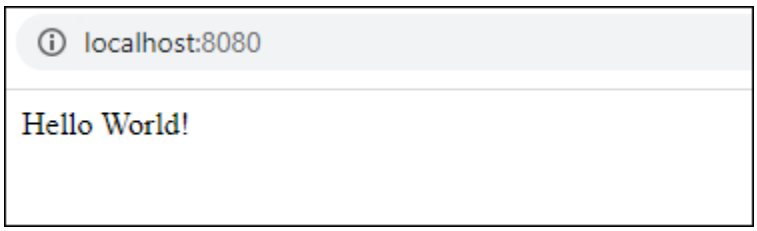
2. Geben Sie den folgenden Befehl ein, um die laufenden Container anzuzeigen.

```
docker container ls -a
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten, das die neuen laufenden Container anzeigt.



3. Um zu bestätigen, dass der Container betriebsbereit ist, öffnen Sie ein neues Browserfenster, und navigieren Sie zu `http://localhost:8080`. Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten. Dies bestätigt, dass Ihr Container auf Ihrem lokalen Computer betriebsbereit ist.



Ihr neu entwickeltes Container-Image ist bereit, auf Ihr Lightsail-Konto übertragen zu werden, damit Sie es in Ihrem Lightsail-Container-Service bereitstellen können. Weitere Informationen finden Sie unter Verschieben und Verwalten von Containter-Images auf Ihre Amazon Lightsail-Container-Services.

(Optional) Schritt 4: Bereinigen der Container, die auf dem lokalen Computer ausgeführt werden

Nachdem Sie nun ein Container-Image erstellt haben, das Sie an Ihren Lightsail-Container-Service verschieben können, ist es an der Zeit, die Container zu bereinigen, die auf Ihrem lokalen Computer ausgeführt werden, nachdem Sie die in diesem Leitfaden beschriebenen Verfahren befolgt haben.

Vervollständigen Sie die folgenden Schritte, um die Container zu bereinigen, die auf Ihrem lokalen Computer ausgeführt werden:

1. Führen Sie den folgenden Befehl aus, um die Container-Services anzuzeigen, die auf Ihrem lokalen Computer ausgeführt werden.

   ```
   docker container ls -a
   ```

   Sie sollten ein Ergebnis ähnlich dem folgenden erhalten, das die Namen der Container auflistet, die auf Ihrem lokalen Computer ausgeführt werden.

   ```
   C:\Users\[redacted]\Documents\Docker\Dockerfiles\mystaticwebsite>docker container ls -a
   CONTAINER ID   IMAGE                  COMMAND                  CREATED          STATUS          PORTS                    NAMES
   62382081e06b   mystaticwebsite:latest   "/bin/sh -c /root/ru…"   6 minutes ago    Up 6 minutes    0.0.0.0:8080->80/tcp   mystaticwebsite
   ```

2. Führen Sie den folgenden Befehl aus, um den ausgeführten Container zu entfernen, den Sie zuvor in diesem Leitfaden erstellt haben. Dadurch wird der Container zwangsweise gestoppt und dauerhaft gelöscht.

   ```
   docker container rm <ContainerName> --force
   ```

Ersetzen Sie im Befehl <ContainerName> den Namen des Containers, den Sie stoppen und löschen möchten.

Beispiel:

```
docker container rm mystaticwebsite --force
```

Der Container, der als Ergebnis dieses Leitfadens erstellt wurde, sollte nun gelöscht werden.

Nächste Schritte nach dem Erstellen von Container-Images

Nachdem Sie Ihre Container-Images erstellt haben, verschieben Sie sie an Ihren Lightsail-Container-Service, wenn Sie bereit sind, diese bereitzustellen. Weitere Informationen finden Sie unter Übertragen und Verwalten von Lightsail-Container-Images.

Themen

- Lightsail-Container-Service-Images verwalten
- Installieren des Lightsail-Container-Service-Plugins
- Privaten Repository-Zugriff von Amazon ECR in Lightsail verwalten

Lightsail-Container-Service-Images verwalten

Wenn Sie eine Bereitstellung in Ihrem Amazon Lightsail-Container-Service erstellen, müssen Sie für jeden Containereintrag ein Quellcontainer-Image angeben. Sie können Images aus einer öffentlichen Registrierung verwenden, z. B. Amazon ECR Public Gallery oder Sie können Images verwenden, die Sie auf Ihrem lokalen Computer erstellen. Erfahren Sie, wie Sie Container-Images von Ihrem lokalen Computer auf den Lightsail-Container-Service schieben. Weitere Informationen finden Sie unter Erstellen von Images für Container-Services.

Inhalt

- Voraussetzungen
- Schieben von Container-Images von Ihrem lokalen Computer an Ihren Container-Service
- Anzeigen von Container-Images, die auf Ihrem Container-Service gespeichert sind
- Löschen von Container-Images, die auf Ihrem Container-Service gespeichert sind

Voraussetzungen

Führen Sie die folgenden Voraussetzungen aus, bevor Sie mit dem Schieben Ihrer Container-Images zu Ihrem Container-Service beginnen:

- Erstellen Sie Ihren Container-Service in Ihrem Lightsail-Konto. Weitere Informationen finden Sie unter Erstellen von Amazon Lightsail-Container-Services.
- Erfahren Sie mehr über die Software, die Sie benötigen, um Ihre eigenen Container-Images auf Ihrem lokalen Computer zu erstellen, und Sie sie dann auf Ihren Lightsail-Container-Service zu schieben. Weitere Informationen finden Sie unter Installieren von Software zur Verwaltung von Container-Images für Ihre Amazon Lightsail-Container-Services.
- Erstellen Sie Container-Images auf Ihrem lokalen Rechner, die Sie an Ihren Lightsail-Container-Service übertragen können. Weitere Informationen finden Sie unter Erstellen von Container-Images für Ihrer Amazon Lightsail-Container-Services.

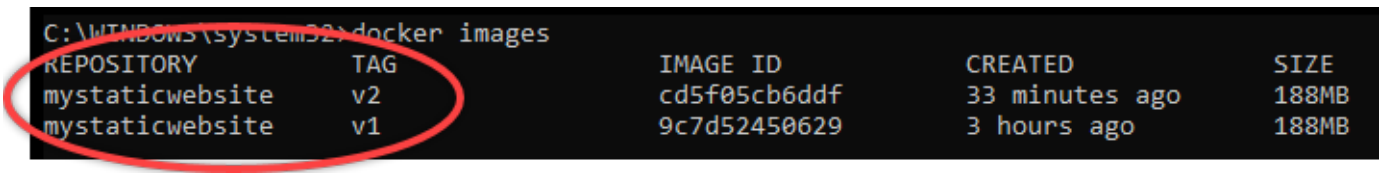
Schieben von Container-Images von Ihrem lokalen Computer an Ihren Container-Service

Führen Sie das folgende Verfahren aus, um Ihre Container-Images an Ihren Container-Service zu übertragen.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie in der Eingabeaufforderung oder im Terminalfenster den folgenden Befehl ein, um die Docker-Images anzuzeigen, die sich derzeit auf Ihrem lokalen Computer befinden.

   ```
   docker images
   ```

3. Suchen Sie im Ergebnis den Namen (Repository-Name) und das Tag des Container-Images, das Sie an den Container-Service senden möchten. Notieren Sie sich dies. Sie benötigen ihn im nächsten Schritt.

4. Geben Sie den folgenden Befehl ein, um das Container-Image auf Ihrem lokalen Computer an den Container-Service zu übertragen.

```
aws lightsail push-container-image --region <Region> --service-
name <ContainerServiceName> --label <ContainerImageLabel> --
image <LocalContainerImageName>:<ImageTag>
```

Ersetzen Sie im Befehl Folgendes:

- *<Region>*in der AWS-Region, in der Ihr Container-Service erstellt wurde.
- *<ContainerServiceName>*durch den Namen Ihres Container-Servicess.
- *<ContainerImageLabel>* mit dem Label, das Sie Ihrem Container-Image geben möchten, wenn es in Ihrem Container-Service gespeichert ist. Geben Sie ein beschreibendes Label an, mit dem Sie die verschiedenen Versionen Ihrer registrierten Container-Images verfolgen können.

  Das Label ist Teil des Container-Image-Namens, der von Ihrem Container-Service generiert wird. Beispiel: Ihr Container-Servicename ist `container-service-1`, die Container-Image-Bezeichnung ist `mystaticsite` und dies ist die erste Version des Container-Images, das Sie verschieben, dann wird der von Ihrem Container-Service generierte Image-Name `:container-service-1.mystaticsite.1`.
- *<LocalContainerImageName>* mit dem Namen des Container-Images, das Sie an Ihren Container-Service senden möchten. Sie haben den Namen des Container-Images im vorherigen Schritt dieses Verfahrens erhalten.
- *<ImageTag>* mit dem Tag des Container-Images, das Sie an Ihren Container-Service senden möchten. Sie haben den Tag des Container-Images im vorherigen Schritt dieses Verfahrens erhalten.

Beispiel:

```
aws lightsail push-container-image --region us-west-2 --service-name myservice --
label mystaticwebsite --image mystaticwebsite:v2
```

Sie sollten ein Ergebnis ähnlich dem folgenden sehen, das bestätigt, dass Ihr Container-Image an den Container-Service übertragen wurde.

```
C:\WINDOWS\system32>aws lightsail push-container-image --service-name myservice --label mystaticwebsite
--image mystaticwebsite:v2

[1B5a355b95: Preparing
[1B0994b087: Preparing
[1B0c904ff3: Preparing
[1B370aa736: Preparing
[1Bf192bbc8: Preparing
[1Bbc0bd923: Preparing
[7BDigest: sha256:3a585ca39bba342e390b39f2fea00bbc20f492c0cda7b923dd766abe31918f3bB/1.96kB
Image "mystaticwebsite:v2" registered.
Refer to this image as ":myservice.mystaticwebsite.2" in deployments.
```

Betrachten Sie den folgenden Abschnitt Anzeigen von Container-Images, die auf Ihrem Container-Service gespeichert sind in diesem Leitfaden, um Ihr Push-Container-Image in Ihrem Container-Service auf der Lightsail-Konsole anzuzeigen.

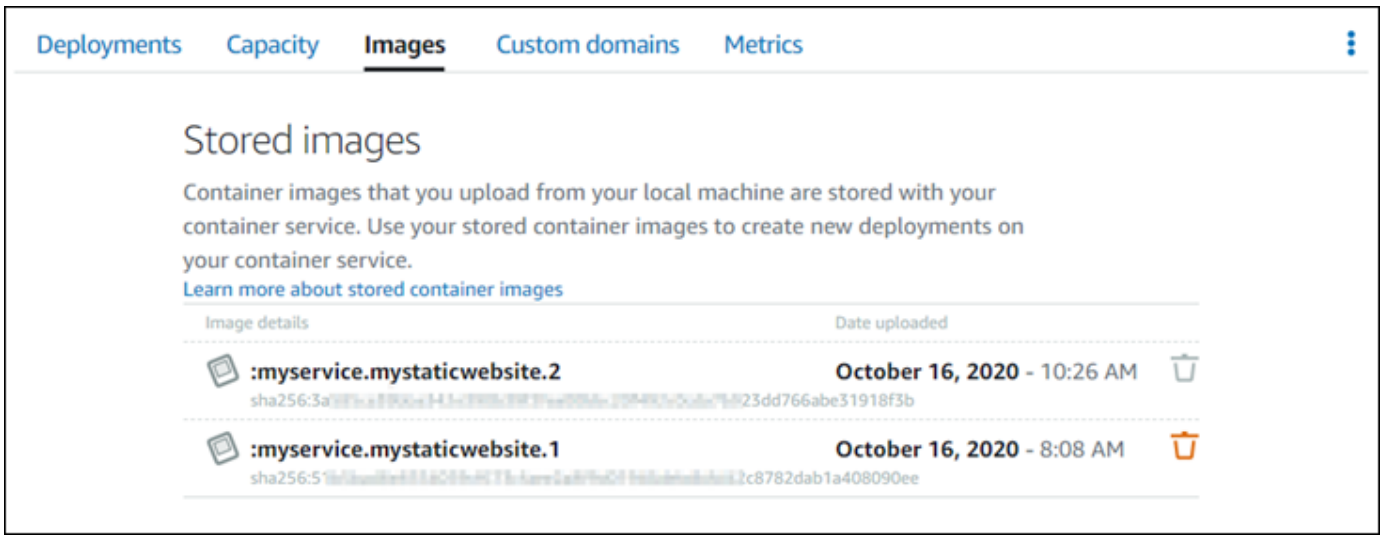
Anzeigen von Container-Images, die auf Ihrem Container-Service gespeichert sind

Führen Sie das folgende Verfahren aus, um Container-Images anzuzeigen, die auf Ihrem Container-Service übertragen wurden und gespeichert werden.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen des Container-Servicess aus, für den Sie die gespeicherten Container-Images anzeigen möchten.
4. Wählen Sie die Registerkarte Images auf der Verwaltungsseite Ihres Container-Servicess aus.

> **Note**
>
> Die Registerkarte Images wird nicht angezeigt, wenn Sie keine Images an Ihren Container-Service übertragen haben. Um die Registerkarte „Images“ für Ihren Container-Service anzuzeigen, müssen Sie zuerst Container-Images an Ihren Service senden.

Die Seite Images listet die Container-Images auf, die an Ihren Container-Service gesendet wurden und derzeit in Ihrem Service gespeichert werden. Container-Images, die in einer aktuellen Bereitstellung verwendet werden, können nicht gelöscht werden und werden mit einem ausgegrauten Löschsymbol aufgelistet.



Sie können Bereitstellungen mit Container-Images erstellen, die in Ihrem Dienst gespeichert sind. Weitere Informationen finden Sie unter Erstellen und Verwalten von Bereitstellungen für Ihre Amazon Lightsail-Container-Services.

Löschen von Container-Images, die auf Ihrem Container-Service gespeichert sind

Führen Sie das folgende Verfahren aus, um Container-Images zu löschen, die auf Ihrem Container-Service übertragen wurden und gespeichert werden.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen des Container-Servicess aus, für den Sie die aktuelle Bereitstellung anzeigen möchten.
4. Wählen Sie die Registerkarte Images auf der Verwaltungsseite Ihres Container-Servicess aus.

> **Note**
>
> Die Registerkarte Images wird nicht angezeigt, wenn Sie keine Images an Ihren Container-Service übertragen haben. Um die Registerkarte „Images“ für Ihren Container-Service anzuzeigen, müssen Sie zuerst Container-Images an Ihren Service senden.

5. Suchen Sie das Container-Image, das Sie löschen möchten und wählen Sie dann das Symbol zum Löschen (Papierkorb) aus.

> **Note**
>
> Container-Images, die in einer aktuellen Bereitstellung verwendet werden, können nicht gelöscht werden, und ihre Löschsymbole sind ausgegraut.

6. Wählen Sie in der angezeigten Bestätigungsaufforderung Ja, löschen um zu bestätigen, dass Sie das gespeicherte Image dauerhaft löschen möchten.

   Ihr gespeichertes Container-Image wird sofort aus Ihrem Container-Service gelöscht.

Installieren des Lightsail-Container-Service-Plugins

Sie können die Amazon Lightsail-Konsole verwenden, um Ihre Lightsail-Container-Services zu erstellen, und Bereitstellungen mithilfe von Container-Images aus einer öffentlichen Online-Registrierung, wie der Amazon ECR Public Gallery zu erstellen. Um eigene Container-Images zu erstellen und sie an Ihren Container-Service zu übertragen, müssen Sie die folgende zusätzliche Software auf demselben Computer installieren, auf dem Sie Ihre Container-Images erstellen möchten:

- Docker – Ermöglicht es Ihnen, eigene Container-Images auszuführen, zu testen und zu erstellen, die Sie dann mit Ihrem Lightsail-Container-Service verwenden können.
- AWS Command Line Interface (AWS CLI) – Ermöglicht es Ihnen, Parameter der von Ihnen erstellten Container-Images anzugeben und diese dann auf Ihre Lightsail-Container-Services zu verschieben. Version 2.1.1 und höher funktioniert mit derLightsailSteuerungs-Plug-In.
- Lightsail-Steuerungs-Plugin (lightsailctl) – Aktiviert die AWS CLI, um auf die Container-Images auf dem lokalen Computer zuzugreifen.

In den folgenden Abschnitten dieses Leitfadens wird beschrieben, wo Sie diese Softwarepakete herunterladen und installieren können. Weitere Informationen zu Container-Services finden Sie unter Container-Services.

Inhalt

- Installieren des lightsailctl-Plugins auf Windows
- Installieren des lightsailctl-Plugins auf macOS
- Installieren des lightsailctl-Plugins auf Linux

Installieren von Docker

Docker ist die Technologie, die Ihnen die Bereitstellung von auf Linux-Containern basierende, verteilte Anwendungen zu entwickeln, auszuführen und zu testen, ermöglicht. Sie müssen die Docker-Software installieren und verwenden, wenn Sie eigene Container-Images erstellen möchten, die Sie dann mit Ihrem Lightsail-Container-Service verwenden. Weitere Informationen finden Sie unter Erstellen von Container-Images für Ihre Lightsail-Container-Services.

Docker ist auf vielen verschiedenen Betriebssystemen verfügbar, darunter die meisten modernen Linux-Verteilungen wie Ubuntu und sogar macOS und Windows. Weitere Informationen zur Installation von Docker unter einem bestimmten Betriebssystem finden Sie im Docker-Installationsleitfaden.

> **Note**
>
> Sie müssen immer die neueste Version von Docker installiert haben. Bei älteren Versionen von Docker ist nicht gewährleistet, dass sie mit dem später in diesem Leitfaden beschriebenen AWS CLI und Lightsail-Steuerungs-Plugin (lightsailctl) funktionieren.

Installieren Sie AWS CLI

Die AWS CLI ist ein Open-Source-Tool, mit der Sie über Befehle in Ihrer Befehlszeile mit AWS-Services, wie z. B. Lightsail, interagieren können. Sie müssen die AWS CLI installieren und verwenden, um Ihre Container-Images, die auf Ihrem lokalen Computer erstellt wurden, auf Ihren Lightsail-Container-Service zu verschieben.

Die AWS CLI ist in den folgenden Versionen verfügbar:

- Version 2.x – Die aktuelle, allgemein verfügbare Version der AWS CLI. Dies ist die neueste Hauptversion der AWS CLI und unterstützt alle aktuellen Funktionen, einschließlich der Möglichkeit, Container-Images auf Ihren Lightsail-Container-Service zu verschieben. Version 2.1.1 und höher funktioniert mit derLightsailSteuerungs-Plug-In.

- Version 1.x Die vorherige Version der AWS CLI, die zwecks Abwärtskompatibilität verfügbar ist. Diese Version unterstützt nicht die Möglichkeit, Ihre Container-Images auf Ihren Lightsail-Container-Service zu verschieben. Daher müssen Sie die AWS CLI-Version installieren, anstatt Version 2 zu verwenden.

Die AWS CLI-Version 2 ist für Linux-, macOS und Windows-Betriebssysteme verfügbar. Anweisungen zur Installation von AWS CLI auf diesen Betriebssystemen finden Sie unter Installieren der AWS CLI-Version 2 im AWS CLI-Benutzerhandbuch.

Installieren desLightsail Steuerungs-Plug-In

Das Lightsail-Steuerung-Plugin (lightsailctl) ist eine leichtgewichtige Anwendung, die AWS CLI erlaubt, auf die Container-Images zuzugreifen, die Sie auf Ihrem lokalen Computer erstellt haben. Es erlaubt Ihnen, Container-Images auf Ihren Lightsail-Container-Service zu verschieben, damit Sie sie für Ihren Dienst bereitstellen können.

Systemanforderungen

- Ein Windows-, macOS - oder Linux-Betriebssystem mit 64-Bit-Unterstützung.
- AWS CLI-Version 2 muss auf Ihrem lokalen Computer installiert sein, um das lightsailctl-Plugin zu verwenden. Weitere Informationen finden Sie im Abschnitt Installieren von AWS CLI weiter oben in diesem Leitfaden.

Verwendung der neuesten Version des lightsailctl-Plugin

Das lightsailctl-Plugin wird gelegentlich mit erweiterter Funktionalität aktualisiert. Jedes Mal, wenn Sie das lightsailctl-Plugin verwenden, führt es eine Überprüfung durch, um zu bestätigen, dass Sie die neueste Version verwenden. Wenn eine neue Version verfügbar ist, werden Sie aufgefordert, auf die neueste Version zu aktualisieren, um die neuesten Funktionen zu nutzen. Wenn Aktualisierungen veröffentlicht werden, müssen Sie die Installation wiederholen, um die aktuelle Version des lightsailctl-Plugins zu erhalten.

In der folgenden Tabelle finden Sie alle Versionen des lightsailctl-Plugins sowie die in den einzelnen Versionen enthaltenen Features und Erweiterungen.

- v1.0.0 (veröffentlicht am 12. November 2020) – Erstveröffentlichung fügt Funktionalität für die AWS CLI-Version 2 hinzu, um Container-Images auf einen Lightsail-Container-Service zu verschieben.

Installieren des lightsailctl-Plugins auf Windows

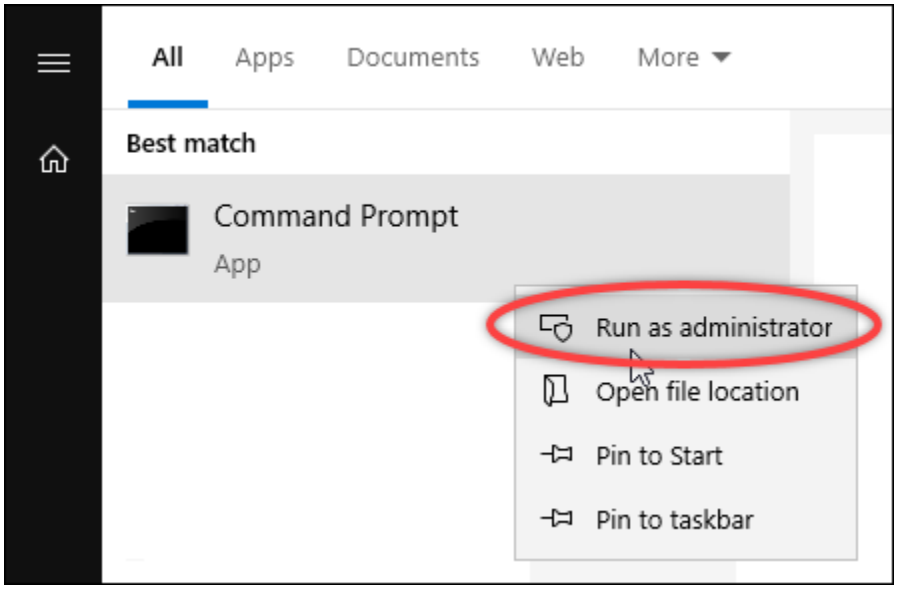
Führen Sie das folgende Verfahren durch, um lightsailctl-Plugin auf Windows zu installieren.

1. Laden Sie die ausführbare Datei über die folgende URL herunter und speichern Sie sie im `C:\Temp\lightsailctl\`-Verzeichnis.

   ```
   https://s3.us-west-2.amazonaws.com/lightsailctl/latest/windows-amd64/
   lightsailctl.exe
   ```

2. Wählen Sie die Windows Start-Schaltfläche aus und suchen Sie dann nach `cmd` .

3. Klicken Sie in den Suchergebnissen mit der rechten Maustaste auf die Anwendung Eingabeaufforderung in den Ergebnissen und wählen Sie Als Administrator ausführen aus.



> **Note**
>
> Möglicherweise wird eine Eingabeaufforderung angezeigt, in der Sie gefragt werden, ob Sie der Eingabeaufforderung erlauben möchten, Änderungen an Ihrem Gerät vorzunehmen. Sie müssenJa auswählen, um mit der Installation fortzufahren.

4. Geben Sie den folgenden Befehl ein, um eine Pfadumgebungsvariable festzulegen, die auf das `C:\Temp\lightsailctl\`-Verzeichnis, in dem Sie das lightsailctl-Plugin gespeichert haben, verweist.

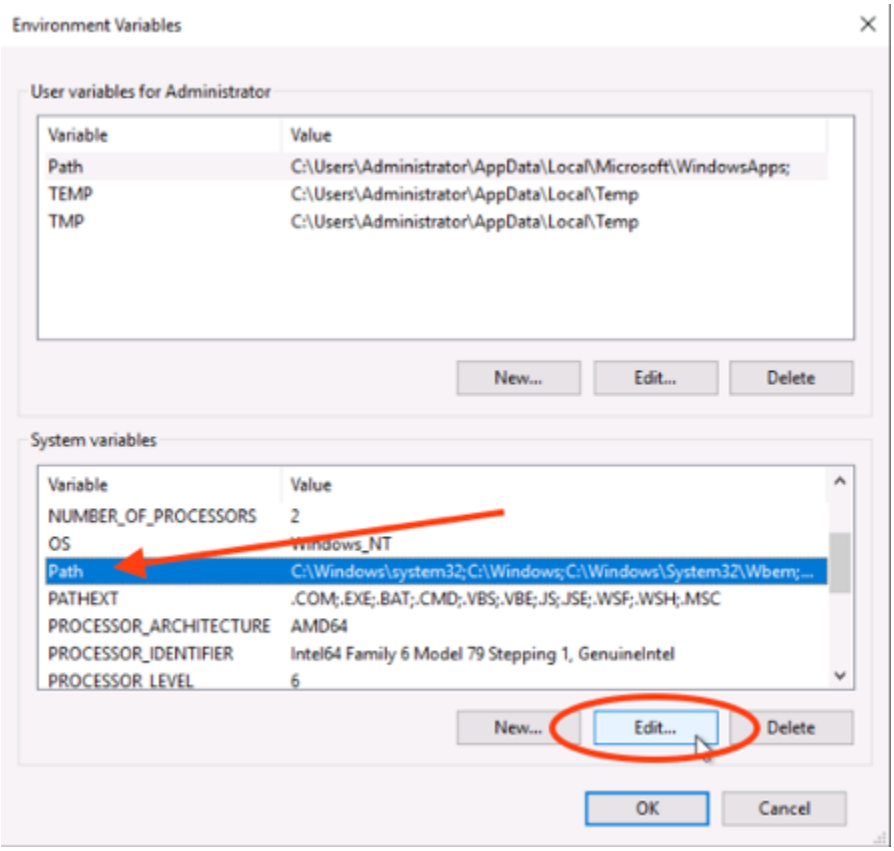
   ```
   setx PATH "%PATH%;C:\Temp\lightsailctl" /M
   ```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

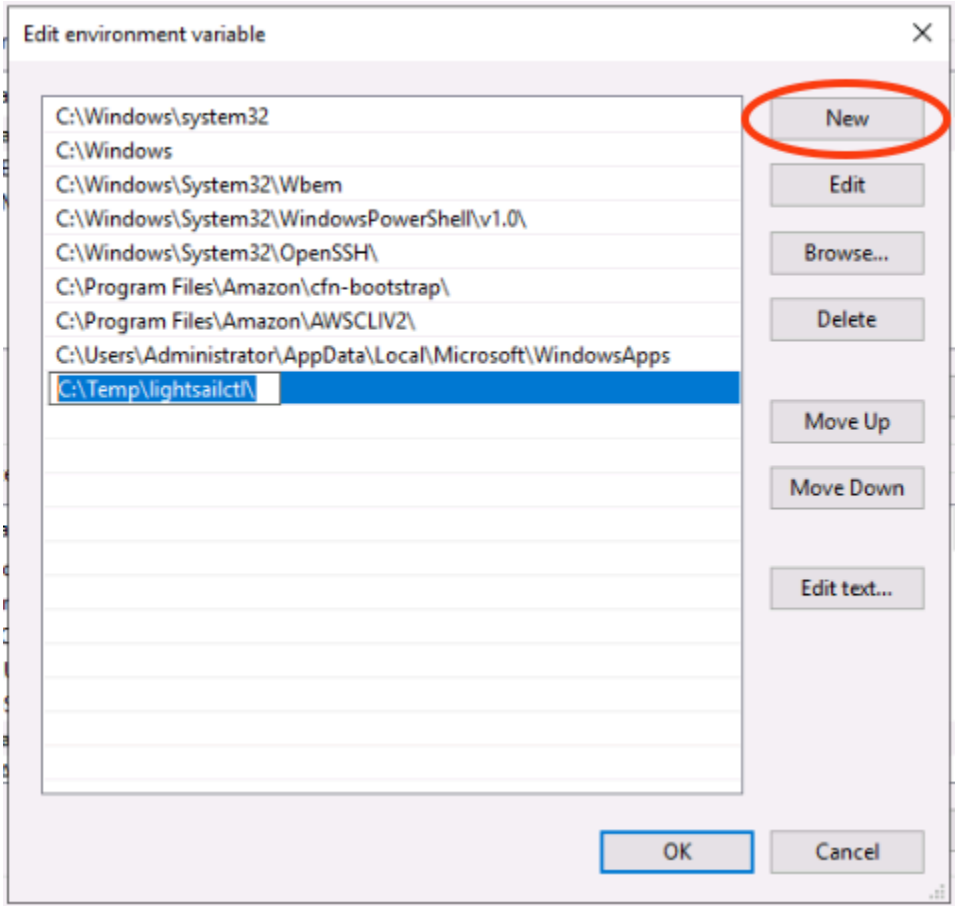
```
C:\WINDOWS\system32>setx PATH "%PATH%;C:\Temp\lightsailctl\" /M

SUCCESS: Specified value was saved.
```

Der Befehl `setx` wird nach mehr als 1 024 Zeichen abgeschnitten. Gehen Sie wie folgt vor, um die Umgebungsvariable „path“ manuell festzulegen, wenn Sie in Ihrem PATH bereits mehrere Variablen gesetzt haben.

1. Klicken Sie im Startmenü auf Systemsteuerung.
2. Wählen Sie System und Sicherheit und dann System.
3. Wählen Sie Choose Advanced system settings (Erweiterte Systemeinstellungen) aus..
4. Öffnen Sie im Dialogfeld Systemeigenschaften die Registerkarte Erweitert und wählen Sie Umgebungsvariablen.
5. Wählen Sie im Feld Systemvariablen des Dialogfelds Umgebungsvariablen die Option Pfad aus.
6. Wählen Sie die Schaltfläche Bearbeiten, die sich unter dem Feld Systemvariablen befindet.



7. Wählen Sie Neu und geben Sie dann den folgenden Pfad ein: `C:\Temp\lightsailctl\`



8. Wählen Sie in drei aufeinanderfolgenden Dialogfeldern OK, und schließen Sie dann das Dialogfeld System.

Sie können jetzt die AWS Command Line Interface (AWS CLI) verwenden, um Container-Images auf Ihren Lightsail-Container-Service zu verschieben. Weitere Informationen finden Sie unter Übertragen und Verwalten von Container-Images.

Installieren des lightsailctl-Plugins auf macOS

Führen Sie eines der folgende Verfahren durch, um lightsailctl-Plugin auf macOS herunterzuladen und zu installieren.

Homebrew herunterladen und installieren

1. Öffnen Sie ein Terminal-Fenster.
2. Geben Sie den folgenden Befehl ein, um das lightsailctl-Plugin herunterzuladen und zu installieren.

```
brew install aws/tap/lightsailctl
```

> **Note**
>
> Weitere Informationen zu Homebrew finden Sie auf der Homebrew-Website.

Manuelles Herunterladen und Installieren

1. Öffnen Sie ein Terminal-Fenster.
2. Geben Sie den folgenden Befehl ein, um das lightsailctl-Plugin herunterzuladen und in den bin-Ordner zu kopieren.

```
curl "https://s3.us-west-2.amazonaws.com/lightsailctl/latest/darwin-amd64/
lightsailctl" -o "/usr/local/bin/lightsailctl"
```

3. Geben Sie den folgenden Befehl ein, um das Plug-In ausführbar zu machen.

```
chmod +x /usr/local/bin/lightsailctl
```

4. Geben Sie den folgenden Befehl ein, um erweiterte Attribute für das Plug-In zu bereinigen.

```
xattr -c /usr/local/bin/lightsailctl
```

Sie können jetzt die AWS CLI verwenden, um Container-Images auf Ihren Lightsail-Container-Service zu verschieben. Weitere Informationen finden Sie unter Übertragen und Verwalten von Container-Images.

Installieren des lightsailctl-Plugins unter Linux

Führen Sie das folgende Verfahren aus, um das Lightsail-Container-Services-Plug-In unter Linux zu installieren.

1. Öffnen Sie ein Terminal-Fenster.
2. Geben Sie den folgenden Befehl ein, um das lightsailctl-Plugin herunterzuladen.

   - Für die AMD-64-Bit-Architekturversion des Plug-Ins:

```
curl "https://s3.us-west-2.amazonaws.com/lightsailctl/latest/linux-amd64/
lightsailctl" -o "/usr/local/bin/lightsailctl"
```

- Für die AMD-64-Bit-Architekturversion des Plug-Ins:

```
curl "https://s3.us-west-2.amazonaws.com/lightsailctl/latest/linux-arm64/
lightsailctl" -o "/usr/local/bin/lightsailctl"
```

3. Geben Sie den folgenden Befehl ein, um das Plug-In ausführbar zu machen.

```
sudo chmod +x /usr/local/bin/lightsailctl
```

Sie können jetzt die AWS CLI verwenden, um Container-Images auf Ihren Lightsail-Container-Service zu verschieben. Weitere Informationen finden Sie unter Übertragen und Verwalten von Container-Images.

Privaten Repository-Zugriff von Amazon ECR in Lightsail verwalten

Amazon Elastic Container Registry (Amazon ECR) ist ein AWS-verwalteter Container-Image-Registry-Service, der private Repositories mit ressourcenbasierten Berechtigungen mithilfe von AWS Identity and Access Management (IAM) unterstützt. Sie können Ihren Amazon Lightsail-Container-Services Zugriff auf Ihre privaten Amazon-ECR-Repositorys gewähren. Anschließend können Sie Images aus Ihrem privaten Repository für Ihre Container-Services bereitstellen.

Sie können den Zugriff für Ihre Lightsail-Container-Services und Ihre Amazon ECR privaten Lightsail-Repositories mithilfe der -Konsole oder der AWS Command Line Interface (AWS CLI). verwalten. Wir empfehlen jedoch die Verwendung der Lightsail-Konsole, da sie den Prozess vereinfacht.

Weitere Informationen zu Container-Services finden Sie unter Container-Services. Weitere Informationen zur Amazon ECR finden Sie unter Sicherheit im Amazon-ECR-Benutzerhandbuch.

Inhalt

- Hinzufügen einer Richtlinie zu einem privaten Repository, das keine Richtlinienanweisung hat
- Hinzufügen einer Richtlinie zu einem privaten Repository, das über eine Richtlinienanweisung verfügt

Erforderliche Berechtigungen

Der Benutzer, der den Zugriff für Lightsail-Container-Services auf private Amazon-ECR-Repositories verwaltet, muss über eine der folgenden Berechtigungsrichtlinien in IAM verfügen. Informationen finden Sie im Abschnitt Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im AWS Identity and Access Management-Benutzerhandbuch.

Gewähren von Zugriff auf jegliche private Amazon-ECR-Repositories

Die folgende Berechtigungsrichtlinie gewährt einem Benutzer die Berechtigung, den Zugriff auf ein beliebiges privates Amazon-ECR-Repository zu konfigurieren.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageEcrPrivateRepositoriesAccess",
            "Effect": "Allow",
            "Action": [
                "ecr:SetRepositoryPolicy",
                "ecr:DescribeRepositories",
                "ecr:DeleteRepositoryPolicy",
                "ecr:GetRepositoryPolicy"
            ],
            "Resource": "arn:aws:ecr:*:AwsAccountId:repository/*"
        }
    ]
}
```

Bearbeiten Sie die Richtlinie, um *AwsAccountId* durch Ihre AWS-Konto-ID zu ersetzen.

Gewähren Sie Zugriff auf ein bestimmtes privates Amazon-ECR-Repository

Die folgende Berechtigungsrichtlinie gewährt einem Benutzer die Berechtigung, den Zugriff auf ein bestimmtes privates Amazon-ECR-Repository in einer bestimmten AWS-Region zu konfigurieren.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageEcrPrivateRepositoriesAccess",
            "Effect": "Allow",
            "Action": [
                "ecr:SetRepositoryPolicy",
                "ecr:DescribeRepositories",
                "ecr:DeleteRepositoryPolicy",
                "ecr:GetRepositoryPolicy"
            ],
            "Resource": "arn:aws:ecr:AwsRegion:AwsAccountId:repository/RepositoryName"
        }
    ]
}
```

Ersetzen Sie in der Richtlinie den folgenden Beispieltext mit Ihrem eigenen:

- *AwsRegion* – Der AWS-Region-Code des privaten Repositorys (z. B. `us-east-1`). Ihr Lightsail-Container-Service muss sich in derselben AWS-Region befinden wie die privaten Repositories, auf die Sie zugreifen möchten.
- *AwsAccountId* – Ihre AWS-Konto-ID-Nummer.
- *RepositoryName* – Der Name des privaten Repositorys, für das Sie den Zugriff verwalten möchten.

Es folgt das Beispiel für die Berechtigungsrichtlinie, die mit Beispielwerten gefüllt ist.

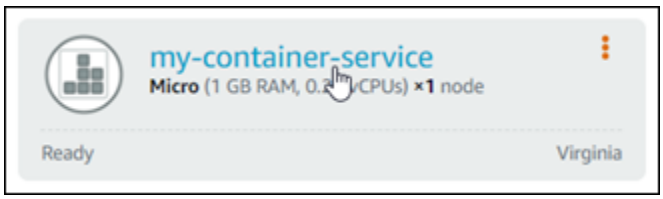
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageEcrPrivateRepositoriesAccess",
            "Effect": "Allow",
            "Action": [
                "ecr:SetRepositoryPolicy",
                "ecr:DescribeRepositories",
                "ecr:DeleteRepositoryPolicy",
                "ecr:GetRepositoryPolicy"
            ],
            "Resource": "arn:aws:ecr:us-east-1:111122223333:repository/my-private-repo"
        }
```

```
    ]
}
```

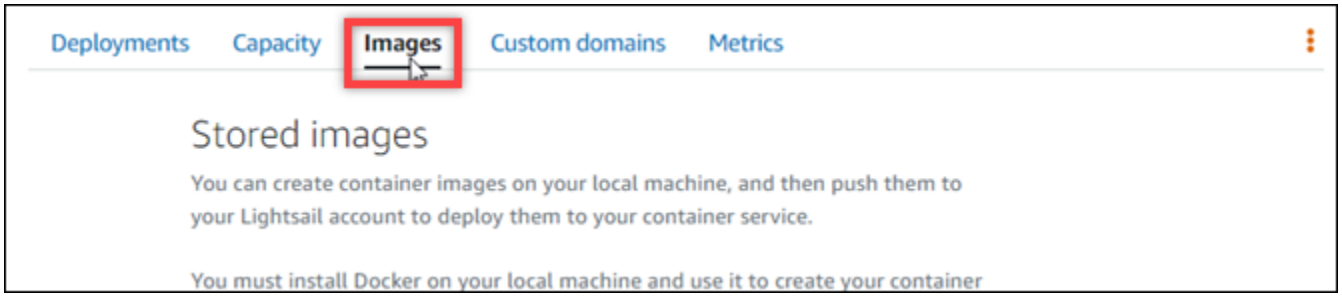
Verwenden der Lightsail-Konsole, um den Zugriff auf private Repositorys zu verwalten

Führen Sie das folgende Verfahren aus, um den Zugriff für einen Lightsail-Container-Service auf ein privates Amazon-ECR-Repository mit der Lightsail-Konsole zu konfigurieren.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen des Container-Services aus, für den Sie den Zugriff auf ein privates Amazon-ECR-Repository konfigurieren möchten.

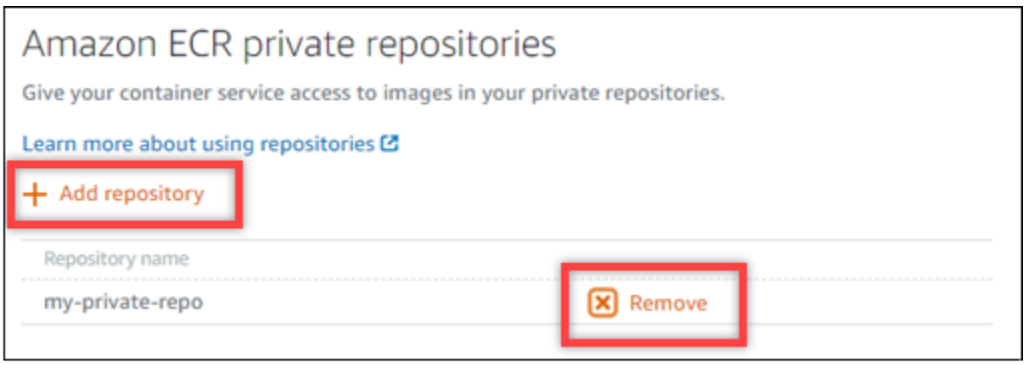


4. Wählen Sie die Registerkarte Images.

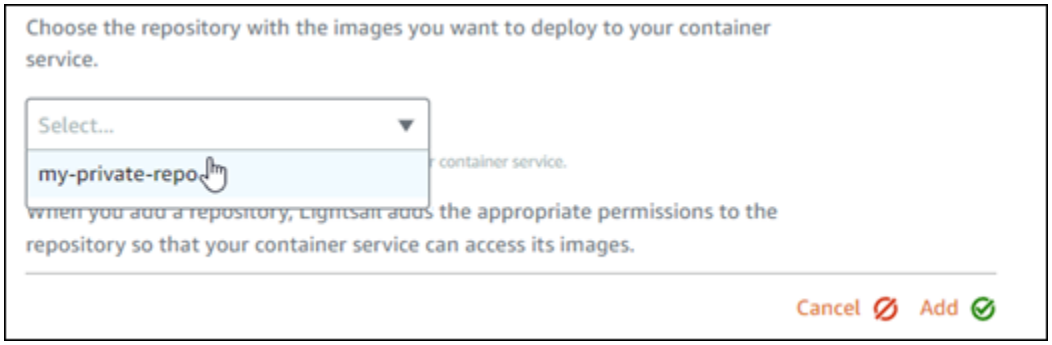


5. Wählen Sie Repository hinzufügen aus, um Ihrem Container-Service Zugriff auf ein privates Amazon-ECR-Repository zu erteilen.

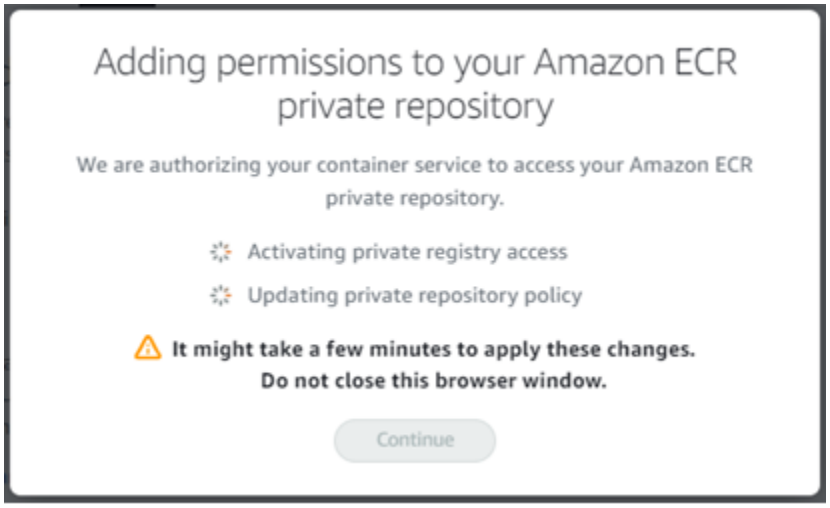
> **Note**
>
> Sie können Entfernen auswählen, um den Zugriff für Ihren Container-Service auf ein zuvor hinzugefügtes privates Amazon-ECR-Repository zu entfernen.



6. Wählen Sie im angezeigten Dropdown-Menü das private Repository aus, auf das Sie zugreifen möchten, und dann Add (Hinzufügen).

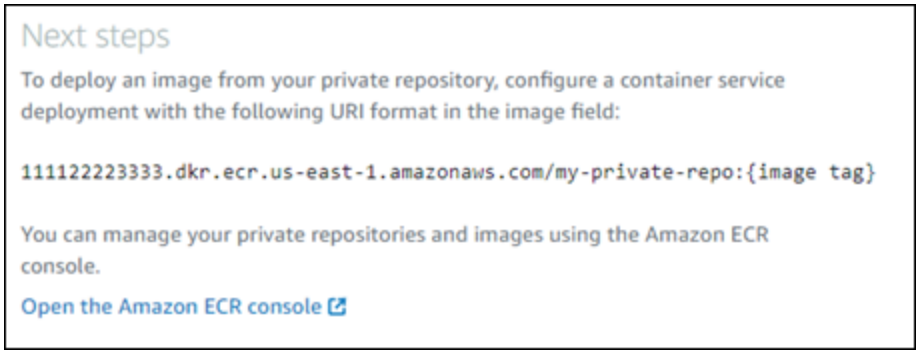


Lightsail braucht einen Moment, um die IAM -Rolle des Amazon-ECR-Image-Pullers für Ihren Container-Service zu aktivieren, welche einen Prinzipal-Amazon-Ressourcennamen (ARN) enthält. Lightsail fügt dann automatisch den IAM-Rollen-Prinzipal-ARN zur Berechtigungsrichtlinie des von Ihnen ausgewählten privaten Amazon-ECR-Repositorys hinzu. Dies gewährt Ihrem Container-Service Zugriff auf das private Repository und seine Images. Schließen Sie das Browserfenster nicht, bis das Modal erscheint und anzeigt, dass der Vorgang abgeschlossen ist, wonach Sie Continue (Weiter) auswählen können.



7. Wählen Sie Continue (Weiter), wenn die Aktivierung abgeschlossen ist.

   Nachdem es ausgewählte private Amazon-ECR-Repository hinzugefügt wurde, wird es im Abschnitt Private Amazon-ECR-Repositorys der Seite aufgeführt. Die Seite enthält Anweisungen zum Bereitstellen eines Image aus dem privaten Repository in Ihrem Lightsail-Container-Service. Um ein Image aus Ihrem privaten Repository zu verwenden, geben Sie das URI-Format an, das auf der Seite beim Erstellen Ihrer Container-Service-Bereitstellung als der Image-Wert angezeigt wird. Ersetzen Sie im URI das Beispiel-*{image tag}* durch das Tag des Image, das Sie bereitstellen möchten. Weitere Informationen finden Sie unter Erstellen und Verwalten von Bereitstellungen für Container-Services.



Verwenden der AWS CLI, um den Zugriff auf private Repositories zu verwalten

Die Verwaltung des Zugriffs für einen Lightsail-Container-Service auf ein privates Amazon-ECR-Repository mithilfe der AWS Command Line Interface (AWS CLI) erfordert die folgenden Schritte:

> **Important**
>
> Wir empfehlen, dass Sie die Lightsail-Konsole verwenden, um den Zugriff eines Lightsail-Container-Services auf ein privates Amazon-ECR-Repository zu verwalten, da sie den Vorgang vereinfacht. Weitere Informationen finden Sie im Abschnitt Verwalten des Zugriffs auf private Repositorys mit der Lightsail-Konsole oben in diesem Leitfaden.

1. Aktivieren oder Deaktivieren der IAM-Rolle des Amazon-ECR-Image-Pullers – Verwenden Sie den AWS CLI-`update-container-service`-Befehl Lightsail für zum Aktivieren oder Deaktivieren der IAM-Rolle des Amazon-ECR-Image-Pullers. Ein Prinzipal-Amazon-Ressourcenname (ARN) wird für die IAM-Rolle des Amazon-ECR-Image-Pullers erstellt, wenn Sie ihn aktivieren. Weitere Informationen finden Sie im Abschnitt Aktivieren oder Deaktivieren der IAM-Rolle des Amazon-ECR-Image-Pullers in diesem Leitfaden.
2. Feststellen, ob Ihr privates Amazon-ECR-Repository über eine Richtlinienerklärung verfügt – Nachdem Sie die IAM-Rolle des Amazon-ECR-Image-Pullers aktiviert haben, müssen Sie bestimmen, ob das private Amazon-ECR-Repository, auf das Sie mit Ihrem Container-Service zugreifen möchten, über eine vorhandene Richtlinienerklärung verfügt. Weitere Informationen finden Sie weiter unten in diesem Leitfaden unter Bestimmen, ob Ihr privates Amazon-ECR-Repository über eine Richtlinienerklärung verfügt.

   Sie fügen den Prinzipal-ARN der IAM-Rolle mit einer der folgenden Methoden zu Ihrem Repository hinzu, je nachdem, ob Ihr Repository über eine vorhandene Richtlinienanweisung verfügt:

   a. Hinzufügen einer Richtlinie zu einem privaten Repository ohne Richtlinienerklärung – Verwenden Sie den AWS CLI-`set-repository-policy`-Befehl für Amazon ECR, um den Prinzipal-ARN der Amazon-ECR-Image-Puller-Rolle für Ihren Container-Service zu einem privaten Repository hinzuzufügen, das über eine vorhandene Richtlinie verfügt. Weitere Informationen finden Sie weiter unten in diesem Leitfaden unter Hinzufügen einer Richtlinie zu einem privaten Repository ohne Richtlinienanweisung.

   b. Hinzufügen einer Richtlinie zu einem privaten Repository mit Richtlinienerklärung – Verwenden Sie den AWS CLI-`set-repository-policy`-Befehl für Amazon ECR, um die Amazon-ECR-Image-Puller-Rolle für Ihren Container-Service zu einem privaten Repository hinzuzufügen, das nicht über eine vorhandene Richtlinie verfügt. Weitere Informationen finden Sie weiter unten in diesem Leitfaden unter Hinzufügen einer Richtlinie zu einem privaten Repository mit Richtlinienanweisung.

Aktivieren oder deaktivieren der IAM-Rolle des Amazon-ECR-Image-Pullers

Führen Sie das folgende Verfahren durch, um die IAM-Rolle des Amazon-ECR-Image-Pullers für IhrenLightsail -Container-Service zu aktivieren oder zu deaktivieren. Sie können die IAM-Rolle des Amazon ECR-Image-Pullers mit dem AWS CLI `update-container-service`-Befehl für Lightsail aktivieren oder deaktivieren. Weitere Informationen finden Sie unter update-container-service in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um einen Container-Service zu aktualisieren und die IAM-Rolle des Amazon-ECR-Image-Pullers zu aktivieren oder zu deaktivieren.

   ```
   aws lightsail update-container-service --service-name ContainerServiceName --
   private-registry-access ecrImagePullerRole={isActive=RoleActivationState} --
   region AwsRegionCode
   ```

   Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

   - *`ContainerServiceName`* – Der Name des Container-Services, für den die IAM-Rolle des Amazon-ECR-Image-Pullers aktiviert oder deaktiviert werden soll.
   - *`RoleActivationState`* – Der Aktivierungsstatus der IAM-Rolle des Amazon-ECR-Image-Pullers. Geben Sie `true` zum Aktivieren der Rolle an, oder `false`, um sie zu deaktivieren.
   - *`AwsRegionCode`* – Der AWS-Region-Code des Container-Service (z. B. `us-east-1`).

   Beispiele:

   - So aktivieren Sie die IAM-Rolle des Amazon-ECR-Image-Pullers:

     ```
     aws lightsail update-container-service --service-name my-container-service --
     private-registry-access ecrImagePullerRole={isActive=true} --region us-east-1
     ```

- So deaktivieren Sie die IAM-Rolle des Amazon-ECR-Image-Pullers:

```
aws lightsail update-container-service --service-name my-container-service --
private-registry-access ecrImagePullerRole={isActive=false} --region us-east-1
```

3. Wenn Sie:

   - Die Amazon-ECR-Image-Puller-Rolle wurde aktiviert – Warten Sie mindestens 30 Sekunden, nachdem Sie die vorherige Antwort erhalten haben. Fahren Sie dann mit dem nächsten Schritt fort, um den Prinzipal-ARN der IAM-Rolle des Amazon-ECR-Image-Pullers für Ihren Container-Service abzurufen.
   - Die Amazon-ECR-Image-Puller-Rolle wurde deaktiviert – Wenn Sie zuvor den Prinzipal-ARN der IAM-Rolle des Amazon-ECR-Image-Pullers zur Berechtigungsrichtlinie Ihres privaten Amazon-ECR-Repositorys hinzugefügt haben, sollten Sie diese Berechtigungsrichtlinie aus Ihrem Repository entfernen. Weitere Informationen finden Sie unter Richtlinienerklärung für ein privates Repository löschen im Amazon-ECR-Benutzerhandbuch.

4. Geben Sie den folgenden Befehl ein, um den Prinzipal-ARN der IAM-Rolle des Amazon-ECR-Image-Pullers für Ihren Container-Service abzurufen.

```
aws lightsail get-container-services --service-name ContainerServiceName --
region AwsRegionCode
```

   Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

   - *ContainerServiceName* – Der Name Ihres Container-Services, für den der Prinzipal-ARN der IAM-Rolle des Amazon-ECR-Image-Pullers abgerufen werden soll.
   - *AwsRegionCode* – Der AWS-Region-Code des Container-Service (z. B. `us-east-1`).

   Beispiel:

```
aws lightsail get-container-services --service-name my-container-service --
region us-east-1
```

   Suchen Sie in der Antwort nach dem Prinzipal-ARN der IAM-Rolle des ECR-Image-Pullers. Wenn eine Rolle aufgeführt ist, kopieren oder notieren Sie sie. Sie benötigen sie für den nächsten Abschnitt dieses Leitfadens. Als Nächstes müssen Sie feststellen, ob eine Richtlinienerklärung auf dem privaten Amazon-ECR-Repository vorhanden ist, auf das Sie mit

Ihrem Container-Service zugreifen möchten. Fahren Sie mit dem Abschnitt Feststellen, ob Ihr privates Amazon-ECR-Repository über eine Richtlinienerklärung verfügt in diesem Leitfaden fort.

Ermitteln, ob Ihr privates Amazon-ECR-Repository eine Richtlinienerklärung hat

Führen Sie die folgenden Schritte aus, um festzustellen, ob Ihr privates Amazon-ECR-Repository über eine Richtlinienerklärung verfügt. Sie können den AWS CLI-`get-repository-policy`-Befehl für Amazon ECR verwenden. Weitere Informationen finden Sie unter update-container-service in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Amazon ECR konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Einrichten von Amazon ECR im Amazon-ECR-Benutzerhandbuch.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um die Richtlinienanweisung für ein bestimmtes privates Repository abzurufen.

   ```
   aws ecr get-repository-policy --repository-name RepositoryName --
   region AwsRegionCode
   ```

   Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

   - *`RepositoryName`* – Der Name des privaten Repositorys, für das Sie den Zugriff für einen Lightsail-Container-Service konfigurieren.
   - *`AwsRegionCode`* – Der AWS-Region-Code des privaten Repositorys (z. B. `us-east-1`).

   Beispiel:

   ```
   aws ecr get-repository-policy --repository-name my-private-repo --region us-east-1
   ```

   Sie sollten eine der folgenden Antworten sehen:

- RepositoryPolicyNotFoundException – Ihr privates Repository hat keine Richtlinienerklärung. Wenn Ihr Repository keine Richtlinienanweisung hat, befolgen Sie die Schritte im Abschnitt Hinzufügen einer Richtlinie zu einem privaten Repository ohne Richtlinienanweisung weiter unten in diesem Leitfaden.

```
C:\>aws ecr get-repository-policy --repository-name my-private-repo

An error occurred (RepositoryPolicyNotFoundException) when calling the GetRepositoryPolicy operation: Repository policy
does not exist for the repository with name 'my-private-repo' in the registry with id '[redacted]'
```

- Eine Repository-Richtlinie wurde gefunden – Ihr privates Repository verfügt über eine Richtlinienerklärung und wird in der Antwort Ihrer Anfrage angezeigt. Wenn Ihr Repository über eine Richtlinienanweisung verfügt, kopieren Sie die vorhandene Richtlinie und befolgen Sie dann die Schritte im Abschnitt Hinzufügen einer Richtlinie zu einem privaten Repository mit einer Richtlinienanweisung weiter unten in diesem Leitfaden.

```
C:\>aws ecr get-repository-policy --repository-name my-private-repo
{
    "registryId": "[redacted]",
    "repositoryName": "my-private-repo",
    "policyText": "{\n  \"Version\" : \"2012-10-17\",\n  \"Statement\" : [ {\n    \"Sid\" : \"AllowUserPushPull\",\n
\"Effect\" : \"Allow\",\n    \"Principal\" : {\n      \"AWS\" : \"arn:aws:iam::[redacted]:user/example-user\"\n    },\
n    \"Action\" : [ \"ecr:BatchGetImage\", \"ecr:BatchCheckLayerAvailability\", \"ecr:CompleteLayerUpload\", \"ecr:GetDo
wnloadUrlForLayer\", \"ecr:InitiateLayerUpload\", \"ecr:PutImage\", \"ecr:UploadLayerPart\" ]\n  } ]\n}"
}
```

Hinzufügen einer Richtlinie zu einem privaten Repository, das keine Richtlinienanweisung hat

Führen Sie das folgende Verfahren aus, um eine Richtlinie zu einem privaten Amazon-ECR-Repository hinzuzufügen, das keine Richtlinienerklärung hat. Die Richtlinie, die Sie hinzufügen, muss den Prinzipal-ARN der IAM-Rolle des Amazon-ECR-Image-Pullers Ihres Lightsail-Container-Services enthalten. Dies gewährt Ihrem Container-Service Zugriff auf die Bereitstellung von Images aus dem privaten Repository.

> **Important**
>
> Lightsail fügt Ihren privaten Amazon-ECR-Repositorys automatisch die Amazon-ECR-Image-Puller-Rolle hinzu, wenn Sie die Lightsail-Konsole zum Konfigurieren des Zugriffs verwenden. In diesem Fall müssen Sie die Amazon-ECR-Image-Puller-Rolle mithilfe des Verfahrens in diesem Abschnitt nicht manuell zu Ihren privaten Repositories hinzufügen. Weitere Informationen finden Sie im Abschnitt Verwalten des Zugriffs auf private Repositorys mit der Lightsail-Konsole oben in diesem Leitfaden.

Sie können mit der AWS CLI eine Richtlinie zu einem privaten Repository hinzufügen. Dazu erstellen Sie eine JSON-Datei, die die Richtlinie enthält, und verweisen dann mit dem `set-repository-policy`-Befehl für Amazon ECR auf diese Datei. Weitere Informationen finden sie unter set-repository-policy in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Amazon ECR konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Einrichten von Amazon ECR im Amazon-ECR-Benutzerhandbuch.

1. Öffnen Sie einen Texteditor und fügen Sie die folgende Richtlinienanweisung in eine neue Textdatei ein.

```
{
  "Version": "2008-10-17",
  "Statement": [
  {
      "Sid": "AllowLightsailPull-ecr-private-repo-demo",
      "Effect": "Allow",
      "Principal": {
        "AWS": "IamRolePrincipalArn"
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ]
    }
  ]
}
```

   Ersetzen Sie im Text *`IamRolePrincipalArn`* durch den Prinzipal-ARN der IAM-Rolle des Amazon-ECR-Image-Pullers Ihres Container-Services, den Sie weiter oben in diesem Leitfaden erhalten haben.

2. Speichern Sie die Datei als `ecr-policy.json` an einem zugänglichen Ort auf Ihrem Computer (z. B. `C:\Temp\ecr-policy.json` unter Windows oder `/tmp/ecr-policy.json` unter macOS oder Linux).

3. Notieren Sie sich den Dateipfadspeicherort der `ecr-policy.json`-Datei die erstellt wurde. Sie werden sie später unten in diesem Verfahren in einem Befehl angeben.
4. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
5. Geben Sie den folgenden Befehl ein, um die Richtlinienanweisung für das private Repository festzulegen, auf das Sie mit Ihrem Container-Service zugreifen möchten.

```
aws ecr set-repository-policy --repository-name RepositoryName --policy-text
 file://path/to/ecr-policy.json --region AwsRegionCode
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *RepositoryName* – Der Name des privaten Repositorys, für das Sie die Richtlinie hinzufügen möchten.
- *Pfad/zu/* – Der Pfad zur `ecr-policy.json`-Datei auf Ihrem Computer, die Sie zuvor in diesem Leitfaden erstellt haben.
- *AwsRegionCode* – Der AWS-Region-Code des privaten Repositorys (z. B. `us-east-1`).

Beispiele:

- Unter Windows:

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file://C:\Temp\ecr-policy.json --region us-east-1
```

- Unter macOS oder Linux:

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file:///tmp/ecr-policy.json --region us-east-1
```

Ihr Container-Service kann jetzt auf Ihr privates Repository und seine Images zugreifen. Um ein Image aus Ihrem Repository zu verwenden, geben Sie den folgenden URI als Image-Wert für Ihre Container-Service-Bereitstellung an. Ersetzen Sie im URI das Beispiel-*Tag* durch das Tag des Image, das Sie bereitstellen möchten. Weitere Informationen finden Sie unter Erstellen und Verwalten von Bereitstellungen für Container-Services.

```
AwsAccountId.dkr.ecr.AwsRegionCode.amazonaws.com/RepositoryName:ImageTag
```

Ersetzen Sie im URI den folgenden Beispieltext mit Ihrem eigenen:

- *AwsAccountId* – Ihre AWS-Konto-ID-Nummer.
- *AwsRegionCode* – Der AWS-Region-Code des privaten Repositorys (z. B. `us-east-1`).
- *RepositoryName* – Der Name des privaten Repositorys, von dem ein Container-Image bereitgestellt werden soll.
- *ImageTag* – Das Tag des Container-Images aus dem privaten Repository, das Sie auf Ihrem Container-Service bereitstellen möchten.

Beispiel:

```
111122223333.dkr.ecr.us-east-1.amazonaws.com/my-private-repo:myappimage
```

Hinzufügen einer Richtlinie zu einem privaten Repository, das über eine Richtlinienanweisung verfügt

Vervollständigen Sie das folgende Verfahren, um eine Richtlinie einem privaten Amazon-ECR-Repository hinzuzufügen, das eine Richtlinienerklärung hat. Die Richtlinie, die Sie hinzufügen, muss die vorhandene Richtlinie und eine neue Richtlinie enthalten, die den Prinzipal-ARN der IAM-Rolle des Amazon-ECR-Image-Pullers Ihres Lightsail-Container-Services enthält. Dies behält die vorhandenen Berechtigungen für Ihr privates Repository bei und gewährt Ihrem Container-Service Zugriff auf die Bereitstellung von Images aus dem privaten Repository.

> **Important**
>
> Lightsail fügt Ihren privaten Amazon-ECR-Repositorys automatisch die Amazon-ECR-Image-Puller-Rolle hinzu, wenn Sie die Lightsail-Konsole zum Konfigurieren des Zugriffs verwenden. In diesem Fall müssen Sie die Amazon-ECR-Image-Puller-Rolle mithilfe des Verfahrens in diesem Abschnitt nicht manuell zu Ihren privaten Repositories hinzufügen. Weitere Informationen finden Sie im Abschnitt Verwalten des Zugriffs auf private Repositorys mit der Lightsail-Konsole oben in diesem Leitfaden.

Sie können mit der AWS CLI eine Richtlinie zu einem privaten Repository hinzufügen. Dazu erstellen Sie eine JSON-Datei, die die vorhandene Richtlinie und die neue Richtlinie enthält. Verweisen Sie dann auf diese Datei mit dem `set-repository-policy`-Befehl für Amazon ECR. Weitere Informationen finden sie unter set-repository-policy in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Amazon ECR konfigurieren, bevor Sie mit diesem Verfahren fortfahren. Weitere Informationen finden Sie unter Einrichten von Amazon ECR im Amazon-ECR-Benutzerhandbuch.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um die Richtlinienanweisung für ein bestimmtes privates Repository abzurufen.

   ```
   aws ecr get-repository-policy --repository-name RepositoryName --
   region AwsRegionCode
   ```

   Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

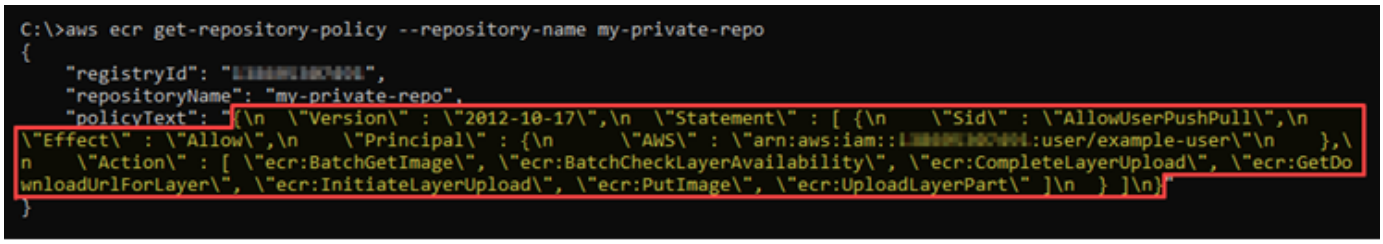
   - *RepositoryName* – Der Name des privaten Repositorys, für das Sie den Zugriff für einen Lightsail-Container-Service konfigurieren.
   - *AwsRegionCode* – Der AWS-Region-Code des privaten Repositorys (z. B. `us-east-1`).

   Beispiel:

   ```
   aws ecr get-repository-policy --repository-name my-private-repo --region us-east-1
   ```

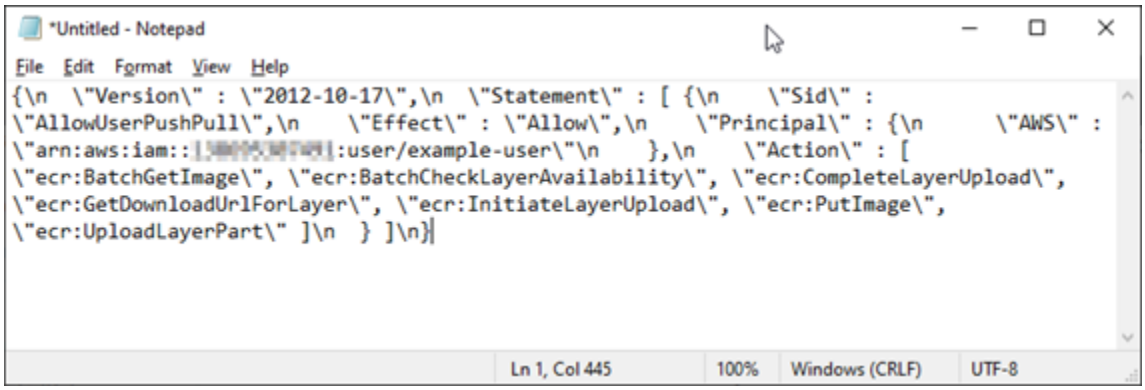
3. Kopieren Sie in der Antwort die vorhandene Richtlinie und fahren Sie mit dem nächsten Schritt fort.

   Sie sollten nur den Inhalt des `policyText` kopieren, der zwischen den doppelten Anführungszeichen erscheint, wie im folgenden Beispiel hervorgehoben.

4. Öffnen Sie einen Texteditor und fügen Sie die vorhandene Richtlinie aus Ihrem privaten Repository ein, das Sie im vorherigen Schritt kopiert haben.

Das Ergebnis sollte wie folgt aussehen:



5. Ersetzen Sie im eingefügten Text \n durch Zeilenumbrüche und löschen Sie das verbleibende \.

   Das Ergebnis sollte wie folgt aussehen:

6. Fügen Sie die folgende Richtlinienanweisung am Ende der Text-Datei ein.

```
,
{
  "Version": "2008-10-17",
  "Statement": [
  {
```

```
      "Sid": "AllowLightsailPull-ecr-private-repo-demo",
      "Effect": "Allow",
      "Principal": {
        "AWS": "IamRolePrincipalArn"
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ]
    }
  ]
}
```

7. Ersetzen Sie im Text *IamRolePrincipalArn* durch den Prinzipal-ARN der IAM-Rolle des Amazon-ECR-Image-Pullers Ihres Container-Services, den Sie weiter oben in diesem Leitfaden erhalten haben.

   Das Ergebnis sollte wie folgt aussehen:

8. Speichern Sie die Datei als `ecr-policy.json` an einem zugänglichen Ort auf Ihrem Computer (z. B. `C:\Temp\ecr-policy.json` unter Windows oder `/tmp/ecr-policy.json` unter macOS oder Linux).
9. Notieren Sie sich den Dateipfadspeicherort der `ecr-policy.json`-Datei. Sie werden sie später unten in diesem Verfahren in einem Befehl angeben.
10. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
11. Geben Sie den folgenden Befehl ein, um die Richtlinienanweisung für das private Repository festzulegen, auf das Sie mit Ihrem Container-Service zugreifen möchten.

```
aws ecr set-repository-policy --repository-name RepositoryName --policy-text
 file://path/to/ecr-policy.json --region AwsRegionCode
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *RepositoryName* – Der Name des privaten Repositorys, für das Sie die Richtlinie hinzufügen möchten.
- *Pfad/zu/* – Der Pfad zur `ecr-policy.json`-Datei auf Ihrem Computer, die Sie zuvor in diesem Leitfaden erstellt haben.
- *AwsRegionCode* – Der AWS-Region-Code des privaten Repositorys (z. B. `us-east-1`).

Beispiele:

- Unter Windows:

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file://C:\Temp\ecr-policy.json --region us-east-1
```

- Unter macOS oder Linux:

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file:///tmp/ecr-policy.json --region us-east-1
```

Sie sollten eine Antwort ähnlich dem folgenden Beispiel erhalten.

Wenn Sie den `get-repository-policy`-Befehl erneut durchführen, sollten Sie die neue zusätzliche Richtlinienerklärung in Ihrem privaten Repository sehen. Ihr Container-Service kann jetzt auf Ihr privates Repository und seine Images zugreifen. Um ein Image aus Ihrem

Repository zu verwenden, geben Sie den folgenden URI als Image-Wert für Ihre Container-Service-Bereitstellung an. Ersetzen Sie im URI das Beispiel-*Tag* durch das Tag des Image, das Sie bereitstellen möchten. Weitere Informationen finden Sie unter Erstellen und Verwalten von Bereitstellungen für Container-Services.

```
AwsAccountId.dkr.ecr.AwsRegionCode.amazonaws.com/RepositoryName:ImageTag
```

Ersetzen Sie im URI den folgenden Beispieltext mit Ihrem eigenen:

- *AwsAccountId* – Ihre AWS-Konto-ID-Nummer.
- *AwsRegionCode* – Der AWS-Region-Code des privaten Repositorys (z. B. `us-east-1`).
- *RepositoryName* – Der Name des privaten Repositorys, von dem ein Container-Image bereitgestellt werden soll.
- *ImageTag* – Das Tag des Container-Images aus dem privaten Repository, das Sie auf Ihrem Container-Service bereitstellen möchten.

Beispiel:

```
111122223333.dkr.ecr.us-east-1.amazonaws.com/my-private-repo:myappimage
```

Erstellen und Verwalten von Container-Services-Bereitstellungen in Lightsail

Erstellen Sie eine Bereitstellung, wenn Sie bereit sind, Container in Ihrem Amazon-Amazon Lightsail-Container-Service zu starten. Bei einer Bereitstellung handelt es sich um eine Reihe von Spezifikationen für die Container, die Sie in Ihrem Dienst starten möchten. Der Container-Service kann jeweils über eine ausgeführte Bereitstellung verfügen, und eine Bereitstellung kann bis zu 10 Containereinträge enthalten. Sie können eine Bereitstellung gleichzeitig erstellen, wenn Sie den Container-Service erstellen, oder Sie können ihn erstellen, nachdem der Dienst ausgeführt wird.

> **Note**
>
> Wenn Sie eine neue Bereitstellung erstellen, verschwinden die vorhandenen Auslastungsmetriken Ihres Container-Services, und es werden nur Metriken für die neue aktuelle Bereitstellung angezeigt.

Weitere Informationen zu Container-Services finden Sie unter Container-Services in Amazon Lightsail.

Inhalt

Voraussetzungen

Führen Sie die folgenden Voraussetzungen aus, bevor Sie mit dem Erstellen einer Bereitstellung in Ihrem Container-Service beginnen:

- Erstellen Sie Ihren Container-Service in Ihrem Lightsail-Konto. Weitere Informationen finden Sie unter Erstellen von Amazon Lightsail-Container-Services.
- Identifizieren Sie die Container-Images, die Sie beim Starten von Containern in Ihrem Container-Service verwenden möchten.

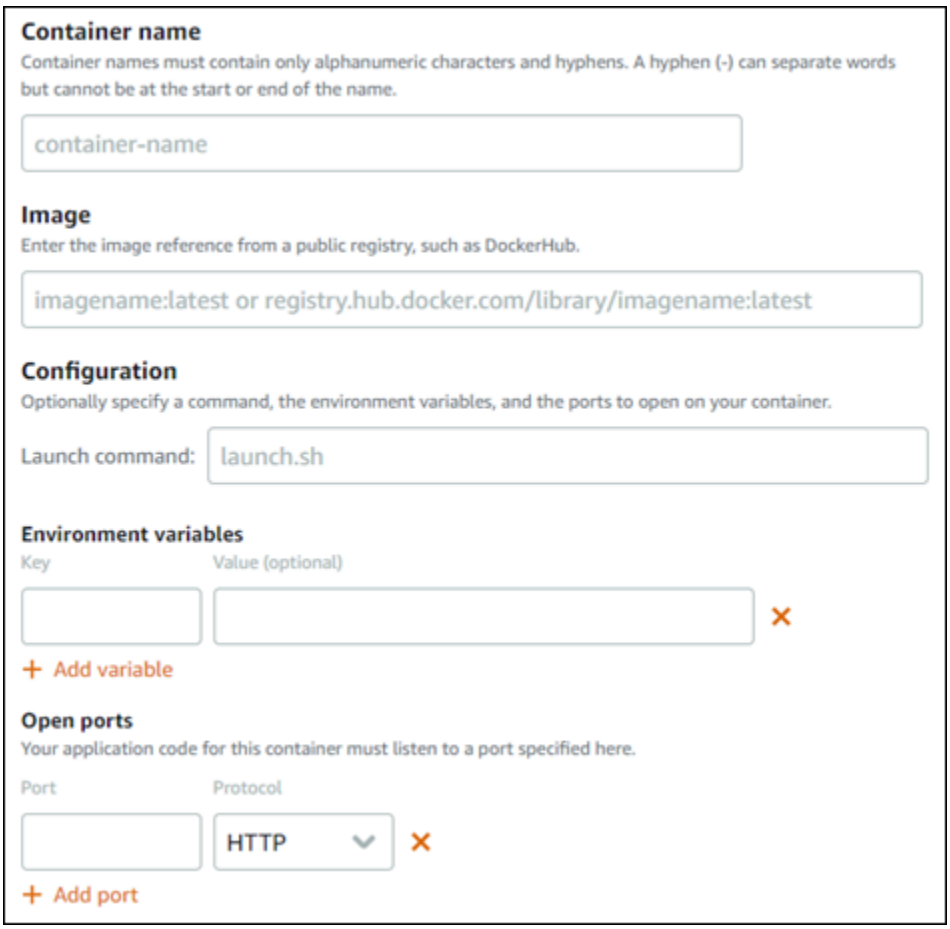
- Suchen von Container-Images in einem öffentlichen Register, z. B. Amazon ECR Public Gallery. Weitere Informationen finden Sie unter Amazon ECR Public Gallery im Benutzerhandbuch für Amazon ECR Public.
- Erstellen Sie Container-Images auf Ihrem lokalen Computer und übertragen Sie sie dann an Ihren Lightsail-Container-Services. Weitere Informationen finden Sie in den folgenden Anleitungen:
  - Installieren von Software zum Verwalten von Container-Images für Ihre Amazon Lightsail-Container-Services
  - Erstellen Sie Container-Service-Images
  - Container-Images verschieben und verwalten

Parameter für die Bereitstellung

In diesem Abschnitt werden die Parameter beschrieben, die Sie für die Containereinträge und den öffentlichen Endpunkt Ihrer Bereitstellung angeben können.

Parameter der Containereingabe

Sie können bis zu 10 Containereinträge in Ihrer Bereitstellung hinzufügen. Jeder Containereintrag verfügt über die folgenden Parameter, die Sie angeben können:



- Containername - Geben Sie für Container den Namen für den Container ein. Alle Container in einer Bereitstellung müssen eindeutige Namen aufweisen und dürfen nur alphanumerische Zeichen und Bindestriche (-) enthalten. Ein Bindestrich kann Wörter trennen, aber er kann sich nicht am Anfang oder Ende des Namens befinden.
- Quellbild — Geben Sie ein Image für den Container an. Sie können Container-Images aus den folgenden Quellen angeben:
  - Ein öffentliches Register, z. B. Amazon ECR Public Gallery, oder ein anderes öffentliches Container-Image-Register.

    Weitere Informationen zu Amazon ECR Public finden Sie unter Was ist Amazon Elastic Container Registry Public? im Benutzerhandbuch von Amazon ECR.
  - Push-Images von Ihrem lokalen Rechner an Ihren Container-Service. Um ein gespeichertes Image anzugeben, wählen Sie Gespeicherte Images auswählen und wählen Sie dann das gewünschte Image aus.

Wenn Sie Container-Images auf Ihrem lokalen Computer erstellen, können Sie sie an Ihren Container-Service senden, um sie beim Erstellen einer Bereitstellung zu verwenden. Weitere Informationen finden Sie unter Erstellen von Container-Images für Ihre Amazon Lightsail-Container-Services und Verschieben und Verwalten von Container-Images auf Ihren Amazon Lightsail-Container-Services.

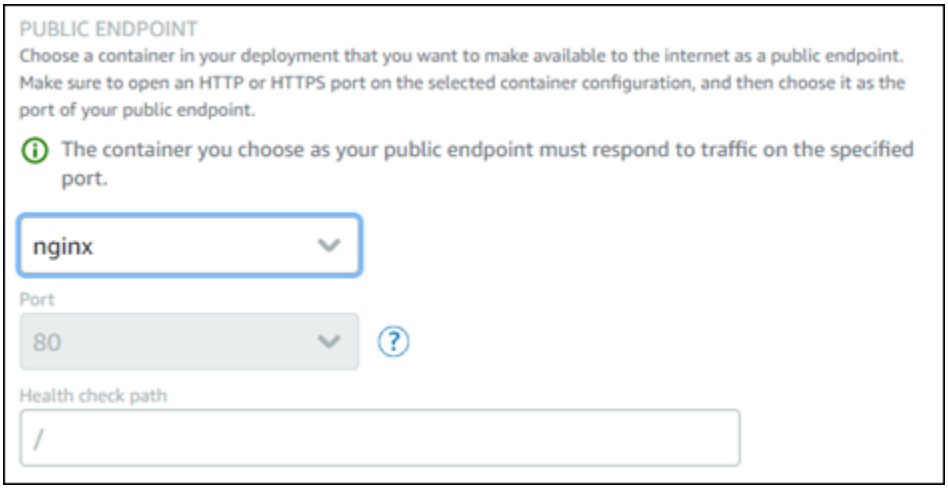
- Startbefehle — Geben Sie einen Startbefehl an, um ein Shell-Skript oder ein Bash-Skript auszuführen, das den Container bei der Erstellung konfiguriert. Ein Befehl starten kann beispielsweise Software hinzufügt oder aktualisiert oder Ihren Container auf andere Weise konfiguriert.
- Umgebungsvariablen — Geben Sie Umgebungsvariablen an, bei denen es sich um Schlüssel-Wert-Parameter handelt, die eine dynamische Konfiguration der Anwendung oder des Skripts bereitstellen, die vom Container ausgeführt werden.
- Öffnen der Ports — Geben Sie die Ports und Protokolle an, die auf dem Container geöffnet werden sollen. Sie können festlegen, dass ein beliebiger Port über HTTP, HTTPS, TCP und UDP geöffnet werden soll. Sie müssen einen HTTP- oder HTTPS-Port für den Container öffnen, den Sie als öffentlichen Endpunkt Ihres Container-Services verwenden möchten. Weitere Informationen finden Sie im Abschnitt in diesem Handbuch.

Parameter für öffentliche Endpunkte

Sie können den Containereintrag in der Bereitstellung angeben, der als öffentlicher Endpunkt Ihres Container-Services dient. Die Anwendung auf dem öffentlichen Endpunktcontainer ist im Internet über eine zufällig generierte Standarddomäne Ihres Container-Services öffentlich zugänglich. Die Standard-Domain ist als `https://<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com` formatiert, wobei *<ServiceName>* der Name Ihres Container-Services ist. *<RandomGUID>* ist eine zufällig generierte globale eindeutige Kennung Ihres Container-Services in der AWS-Region für Ihr Lightsail-Konto und *<AWSRegion>* ist die AWS-Region, in der der Container-Service erstellt wurde. Der öffentliche Endpunkt von Lightsail-Container-Services unterstützt nur HTTPS und unterstützt keinen TCP- oder UDP-Datenverkehr. Nur ein Container kann der öffentliche Endpunkt für einen Dienst sein. Stellen Sie also sicher, dass Sie den Container, der das Frontend Ihrer Anwendung hostet, als öffentlichen Endpunkt auswählen, während auf die restlichen Container intern zugegriffen werden kann.

> **Note**
>
> Sie können Ihren eigenen benutzerdefinierten Domänennamen mit Ihrem Container-Service verwenden. Weitere Informationen finden Sie unter Aktivieren und Verwalten benutzerdefinierter Domänen für Ihre Amazon Lightsail-Container-Services.

Der öffentliche Endpunkt Ihrer Bereitstellung und der Container-Service verfügen über die folgenden Parameter, die Sie angeben können:



- Endpunkt-Container — Wählen Sie den Namen des Containers in Ihrer Bereitstellung aus, der als öffentlicher Endpunkt Ihres Container-Services dient. Im Dropdown-Menü werden nur die Container aufgeführt, deren HTTP- oder HTTPS-Port in der Bereitstellung geöffnet ist.
- Port — Wählen Sie den HTTP- oder HTTPS-Port aus, der für den öffentlichen Endpunkt verwendet werden soll. Im Dropdown-Menü werden nur die HTTP- und HTTPS-Ports aufgeführt, die auf dem ausgewählten Container geöffnet sind. Wählen Sie einen HTTP-Port aus, wenn der ausgewählte Container nicht so konfiguriert ist, dass er beim ersten Start eine HTTPS-Verbindung unterstützt.

> **Note**
>
> Die Standarddomäne für Ihren Container-Service verwendet standardmäßig HTTPS, selbst wenn Sie einen HTTP-Port als öffentlichen Endpunktport auswählen. Dies liegt daran, dass der Load Balancer Ihres Containerservices standardmäßig für HTTPS konfiguriert ist, aber HTTP verwendet, um eine Verbindung mit Ihren Containern herzustellen.
> Der Load Balancer Ihres Containerservices stellt über HTTP eine Verbindung zu Ihren Containern her, stellt jedoch den Benutzern mithilfe von HTTPS Inhalte zur Verfügung.

- Health check path (Pfad für die Zustandsprüfung) – Geben Sie einen Pfad auf dem ausgewählten öffentlichen Endpunktcontainer an, in dem der Load Balancer des Containerservices regelmäßig überprüft, ob er fehlerfrei ist.
- Erweiterte Zustandsprüfungseinstellungen – Sie können die folgenden Einstellungen für die Integritätsprüfung für den ausgewählten öffentlichen Endpunkt-Container konfigurieren:
  - Timeout für Zustandsprüfung in Sekunden – Die Wartezeit in Sekunden, bis eine Antwort eingeht. Wenn während dieser Zeit keine Antwort eingeht, schlägt der Gesundheitscheck fehl. Sie können 2–60 Sekunden eingeben.
  - Intervall für Zustandsprüfungen in Sekunden – Das ungefähre Intervall in Sekunden zwischen den Zustandsprüfungen des Containers. Sie können 5–300 Sekunden eingeben.
  - Zustandsprüfungscodes für – Die HTTP-Codes, die verwendet werden, um einen Container auf eine erfolgreiche Antwort zu überprüfen. Sie können Werte zwischen 200 und 499 angeben. Sie können mehrere Werte angeben (z. B. 200, 202) oder einen Wertebereich (z. B. 200–299).
  - Zustandsprüfung, fehlerhafter Schwellenwert – Die Anzahl aufeinanderfolgender Erfolge für Zustandsprüfungen, die erforderlich sind, bevor der Container in den fehlerfreien Zustand versetzt wird.
  - Zustandsprüfung, fehlerhafter Schwellenwert – Die Anzahl aufeinanderfolgender Erfolge für Zustandsprüfungen, die erforderlich sind, bevor der Container in den fehlerhaften Zustand versetzt wird.

Private Domain

Alle Container-Services verfügen auch über eine private Domäne mit einer `<ServiceName>.service.local`-Formatierung, in dem der Name Ihres Container-Servicess `<ServiceName>` lautet. Verwenden Sie die private Domain, um von einer anderen Ihrer Lightsail-Ressourcen in derselben AWS-Region wie Ihr Service auf Ihren Container-Service zuzugreifen. Die private Domäne ist die einzige Möglichkeit, auf Ihren Container-Service zuzugreifen, wenn Sie in der Bereitstellung Ihres Dienstes keinen öffentlichen Endpunkt angeben. Eine Standarddomäne wird für Ihren Container-Service generiert, auch wenn Sie keinen öffentlichen Endpunkt angeben, aber es wird eine `404 No Such Service`-Fehlermeldung anzeigen, wenn Sie versuchen, zu ihm zu navigieren.

Um mit der privaten Domäne Ihres Container-Services auf einen bestimmten Container zuzugreifen, müssen Sie den offenen Port des Containers angeben, der Ihre Verbindungsanforderung akzeptiert. Sie tun dies, indem Sie die Domain Ihrer Anfrage als `<ServiceName>.service.local:<PortNumber>`, in dem `<ServiceName>`. Dies ist der

Name Ihres Container-Dienstes und *<PortNumber>* ist der offene Port des Containers, mit dem Sie eine Verbindung herstellen möchten. Wenn Sie beispielsweise eine Bereitstellung für Ihren Container-Service mit dem Namen`container-service-1`, und Sie geben einen Redis-Container mit Port 6379 öffnen, sollten Sie die Domain Ihrer Anfrage als *`container-service-1`*`.service.local:`*`6379`* aus.

Kommunikation zwischen Containern

Mithilfe von Umgebungsvariablen können Sie die Kommunikation zwischen Containern innerhalb desselben Containerservices, Containern innerhalb verschiedener Containerservices oder zwischen einem Container und anderen Ressourcen (z. B. zwischen einem Container und einer verwalteten Datenbank) öffnen.

Um die Kommunikation zwischen Containern innerhalb desselben Containerservices zu öffnen, fügen Sie Ihrer Containerbereitstellung eine Umgebungsvariable hinzu, die auf `localhost` verweist, wie im folgenden Beispiel gezeigt.

Um die Kommunikation zwischen Containern zu öffnen, die sich in verschiedenen Containerservices befinden, fügen Sie Ihrer Containerbereitstellung eine Umgebungsvariable hinzu, die auf die private Domain (z. B. `container-service-1.service.local`) des anderen Containerservices verweist, wie im folgenden Beispiel gezeigt.

Um die Kommunikation zwischen Containern und anderen Ressourcen zu öffnen, fügen Sie Ihrer Containerbereitstellung eine Umgebungsvariable hinzu, die auf die öffentliche Endpunkt-URL der Ressource verweist. Beispielsweise ist der öffentliche Endpunkt einer von Lightsail verwalteten Datenbank normalerweise `ls-123abc.czoexamplezqi.us-west-2.rds.amazonaws.com`. Verweisen Sie also in der Umgebungsvariablen, wie im folgenden Beispiel gezeigt.

Containerprotokolle

Jeder Container in Ihrer Bereitstellung generiert ein Protokoll. Die Containerprotokolle stellen die stdout- und stderr-Streams von Prozessen, die innerhalb des Containers ausgeführt werden. Greifen Sie regelmäßig auf die Protokolle Ihrer Container zu, um deren Vorgänge zu diagnostizieren. Weitere Informationen finden Sie unter Anzeigen der Containerprotokolle Ihrer Amazon Lightsail-Container-Services.

Bereitstellungs-Versionen

Jede Bereitstellung, die Sie in Ihrem Amazon Lightsail-Container-Service erstellen, wird als Bereitstellungsversion gespeichert. Wenn Sie die Parameter einer vorhandenen Bereitstellung ändern, werden die Container erneut für Ihren Dienst bereitgestellt, und die geänderte Bereitstellung führt zu einer neuen Bereitstellungsversion. Die neuesten 50 Bereitstellungsversionen für jeden Container-Service werden gespeichert. Sie können jede der 50 Bereitstellungsversionen verwenden, um eine neue Bereitstellung im selben Container-Service zu erstellen. Weitere Informationen finden Sie unter Anzeigen und Verwalten von Bereitstellungsversionen Ihrer Amazon Lightsail-Container-Services.

Bereitstellungsstatus

Nachdem Ihre Bereitstellung erstellt wurde, kann sie einen der folgenden Status aufweisen:

- Aktivierung — Ihre Bereitstellung wird aktiviert, und Ihre Container werden erstellt.
- Aktiv — Ihre Bereitstellung wurde erfolgreich erstellt und wird derzeit auf Ihrem Container-Service ausgeführt.
- Inaktiv — Ihre zuvor erfolgreich erstellte Bereitstellung wird nicht mehr auf Ihrem Container ausgeführt.
- Fehlgeschlagen — Ihre Bereitstellung ist fehlgeschlagen, da ein oder mehrere der in der Bereitstellung angegebenen Container nicht gestartet werden konnten.

Fehler bei der Bereitstellung

Wenn ein oder mehrere Container in Ihrer Bereitstellung nicht gestartet werden können. Wenn Ihre Bereitstellung fehlschlägt und eine frühere Bereitstellung auf Ihrem Container-Service ausgeführt wird, behält der Container-Service die vorherige Bereitstellung als aktive Bereitstellung bei. Wenn keine vorherige Bereitstellung vorhanden ist, bleibt der Container-Service im Bereitschaftszustand, ohne dass derzeit aktive Bereitstellung vorhanden ist.

Zeigen Sie die Containerprotokolle der fehlgeschlagenen Bereitstellung an, um Fehler zu diagnostizieren und zu beheben. Weitere Informationen finden Sie unter Anzeigen der Containerprotokolle Ihrer Amazon Lightsail-Container-Services.

Anzeigen der Container-Service-Bereitstellung

Führen Sie das folgende Verfahren aus, um die derzeitige Bereitstellung Ihres Lightsail-Container-Services anzuzeigen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen des Container-Services aus, für den Sie die aktivierten benutzerdefinierten Domänen anzeigen möchten.
4. Wählen Sie die Registerkarte Bereitstellungen auf der Verwaltungsseite Ihres Container-Services aus.

   DieBereitstellungen listet Ihre aktuellen Bereitstellungs- und Bereitstellungsversionen auf. Beide Abschnitte der Seite sind leer, wenn Sie keine Bereitstellung in Ihrem Container-Service erstellt haben.

Erstellen oder Ändern der Container-Service-Bereitstellung

Führen Sie die folgenden Schritte aus, um eine Bereitstellung für Ihren Lightsail-Container-Service zu erstellen oder zu ändern. Unabhängig davon, ob Sie eine neue Bereitstellung erstellen oder eine vorhandene Version ändern, Ihr Container-Service speichert jede Bereitstellung als neue Bereitstellungsversion. Weitere Informationen finden Sie unter Anzeigen und Verwalten von Bereitstellungsversionen Ihrer Amazon Lightsail-Container-Services.

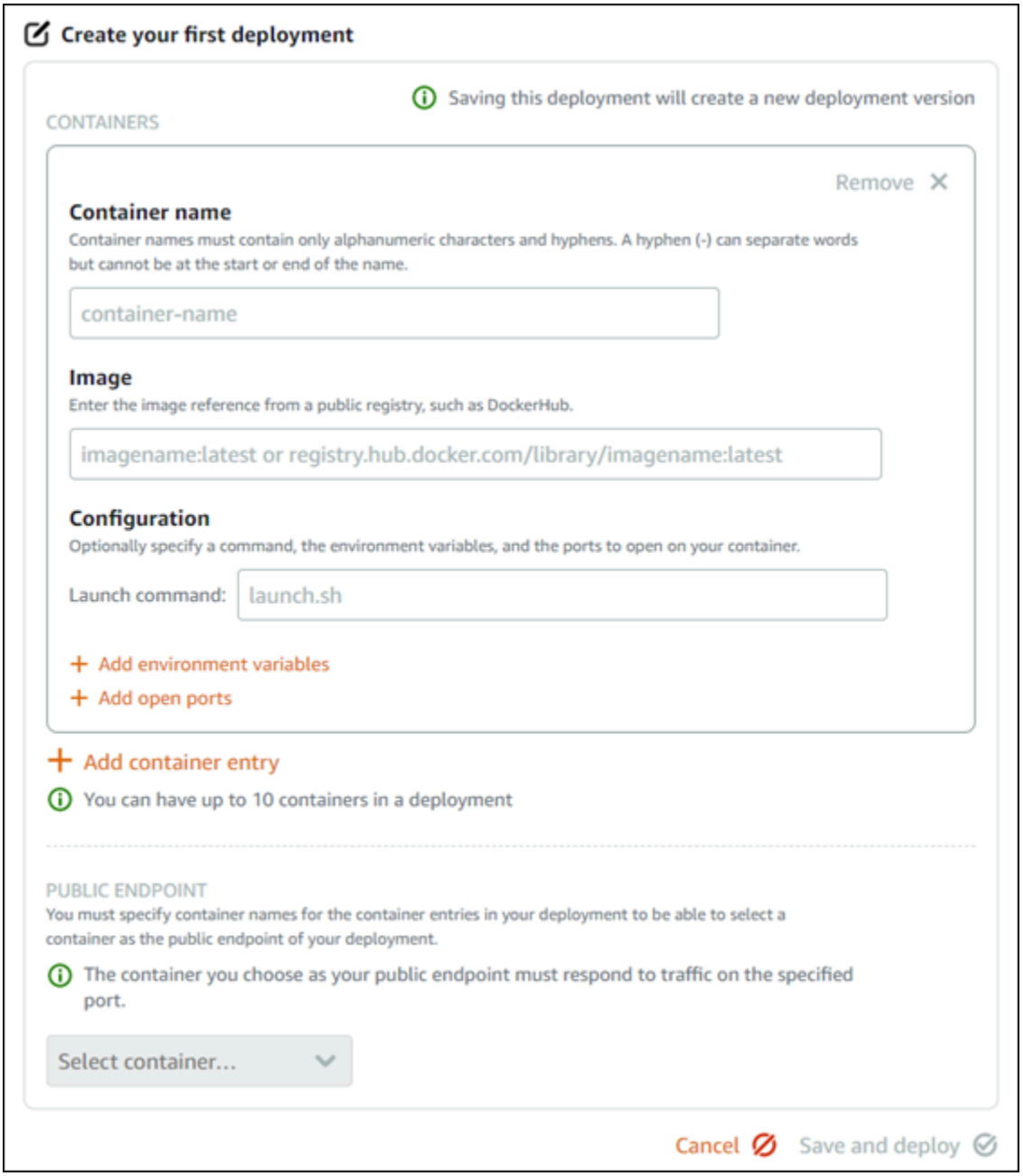
1. Melden Sie sich an der Lightsail-Konsole an.

2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen des Container-Services aus, für den Sie eine Container-Service-Bereitstellung erstellen oder ändern möchten.
4. Wählen Sie die Registerkarte Bereitstellungen auf der Verwaltungsseite Ihres Container-Services aus.

   DieBereitstellungen listet ggf. Ihre aktuellen Bereitstellungs- und Bereitstellungsversionen auf.
5. Wählen Sie eine der folgenden Optionen:

   - Wenn Ihr Container-Service über eine vorhandene Bereitstellung verfügt, wählen Sie Ändern der Bereitstellung aus.
   - Wenn Ihr Container-Service über keine Bereitstellung verfügt, wählen Sie Eine Bereitstellung auswählen aus.

     Das Bereitstellungsformular wird geöffnet, in dem Sie vorhandene Bereitstellungsparameter bearbeiten oder neue Bereitstellungsparameter eingeben können.



6. Geben Sie die Parameter Ihrer Bereitstellung ein. Weitere Informationen zu den Bereitstellungsparametern, die Sie angeben können, finden Sie unter dem Abschnitt Parameter für die Bereitstellung weiter oben in diesem Leitfaden.
7. Wählen SieContainereintrag hinzufügen, um Ihrer Bereitstellung mehr als einen Containereintrag hinzuzufügen. Sie können über bis zu 10 Containereinträge verfügen.
8. Wählen Sie den Containereintrag Ihrer Bereitstellung aus, der als Container-Service für öffentliche Endpunkte dienen soll. Dies umfasst die Angabe des HTTP- oder HTTPS-Ports, des Zustandsprüfpfads für den ausgewählten Containereintrag und erweiterte Einstellungen für die

Zustandsprüfung. Weitere Informationen finden Sie unter Parameter für öffentliche Endpunkte weiter oben in diesem Leitfaden.

9. Wenn Sie mit der Eingabe der Parameter Ihrer Bereitstellung fertig sind, wählen Sie Speichern und Bereitstellen, um die Bereitstellung auf Ihrem Container-Service zu erstellen.

   Der Status Ihres Container-Services ändert sich auf Bereitstellen, während Ihre Bereitstellung in einer Kiste ausgeführt wird. Nach einigen Augenblicken ändert sich der Status Ihres Container-Services je nach Status Ihrer Bereitstellung in einen der folgenden Optionen:

   - Wenn Ihre Bereitstellung erfolgreich ist, ändert sich der Status Ihres Container-Services auf Ausführen und der Status der Bereitstellung auf Aktiv. Wenn Sie einen öffentlichen Endpunkt in Ihrer Bereitstellung konfiguriert haben, ist der als öffentlicher Endpunkt ausgewählte Container über die Standarddomäne Ihres Container-Services verfügbar.
   - Wenn Ihre Bereitstellung fehlschlägt und eine frühere Bereitstellung auf Ihrem Container-Service ausgeführt wird, ändert sich der Status Ihres Container-Services auf Ausführen und Ihr Container-Service behält die vorherige Bereitstellung als aktive Bereitstellung bei. Wenn es keine vorherige Bereitstellung gibt, ändert sich der Status Ihres Container-Services auf Bereit, ohne derzeit aktive Bereitstellung. Zeigen Sie die Containerprotokolle der fehlgeschlagenen Bereitstellung an, um Fehler zu diagnostizieren und zu beheben. Weitere Informationen finden Sie unter „Anzeigen der Containerprotokolle Ihrer Amazon Lightsail-Container-Services“.

Themen

Ändern der Kapazität Ihres Lightsail-Container-Services

Die Kapazität Ihres Amazon Lightsail-Container-Services besteht aus seiner Größe und Leistung. Die Skalierung gibt die Anzahl der Computing-Knoten in Ihrem Container-Service an, und die Stromversorgung gibt den Speicher und die vCPUs der einzelnen Knoten in Ihrem Dienst an. Sie wählen die Skalierung basierend auf der Anzahl der Knoten aus, die Ihren Dienst betreiben soll und die für eine bessere Verfügbarkeit und höhere Kapazität erforderlich ist

Wenn Sie die Vorgehensweise in diesem Leitfaden befolgen, können Sie die Leistung und Skalierung Ihres Container-Services jederzeit dynamisch und ohne Ausfallzeiten erhöhen, wenn Sie feststellen,

dass er unterprovisioniert ist, oder verringern, wenn Sie feststellen, dass er überprovisioniert ist. Lightsail verwaltet die Kapazitätsänderung automatisch zusammen mit Ihrer aktuellen Bereitstellung.

> **Note**
>
> Wenn Sie eine neue Bereitstellung erstellen, verschwinden die vorhandenen Auslastungsmetriken Ihres Container-Servicess, und es werden nur Metriken für die neue aktuelle Bereitstellung angezeigt.

Weitere Informationen zu Container-Services finden Sie unter Container-Services.

Ändern Sie die Kapazität Ihres Container-Services

Vervollständigen Sie den folgenden Vorgang, um Ihren Lightsail-Container-Service zu löschen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen des Container-Services aus, für den Sie die Kapazität ändern möchten.
4. Wählen Sie die Registerkarte Kapazität auf der Verwaltungsseite Ihres Container-Services aus.

   Der aktuelle Stromverbrauch, die Skalierung und der monatliche Preis Ihres Container-Services wird in der Seite Kapazität angezeigt.
5. Wählen Sie Ändern der Kapazität, um die Stromversorgung und die Skalierung auf etwas anderes zu ändern.
6. Wählen Sie in der angezeigten Bestätigungsmeldung Ja, fortfahren, um zu bestätigen, dass eine Änderung der Kapazität Ihres Container-Services die aktuelle Bereitstellung erneut bereitstellen wird.
7. Wählen Sie die neue Leistung und Skalierung Ihres Container-Services.
8. Klicken Sie aufJa, bewerben, um die neue Kapazität auf Ihren Container-Service anzuwenden.

   Der Status Ihres Container-Services ändert sich in Wird aktualisiert. Nach einigen Augenblicken ändert sich der Status Ihres Dienstes in Aktiviert und es beginnt, unter seiner neuen Kapazität zu arbeiten.

Verwalten von Versionen zur Bereitstellung eines Lightsail-Container-Services

Jede Bereitstellung, die Sie in Ihrem Amazon Lightsail-Container-Service erstellen, wird als Bereitstellungsversion gespeichert. Wenn Sie die Parameter einer vorhandenen Bereitstellung ändern, werden die Container erneut für Ihren Dienst bereitgestellt, und die geänderte Bereitstellung führt zu einer neuen Bereitstellungsversion. Die neuesten 50 Bereitstellungsversionen für jeden Container-Service werden gespeichert. Sie können jede der 50 Bereitstellungsversionen verwenden, um eine neue Bereitstellung im selben Container-Service zu erstellen. In diesem Handbuch zeigen wir Ihnen, wie Sie die Bereitstellungsversionen Ihres Containerservices anzeigen und verwalten können.

Weitere Informationen zu Container-Services finden Sie unter Container-Services.

Bereitstellungsstatus

Nach der Erstellung kann jede Ihrer Bereitstellungsversionen einen der folgenden Status aufweisen:

- Bereitstellen (Aktivieren) – Die Bereitstellung wird gestartet.
- Aktiv – Ihre Bereitstellung wurde erfolgreich erstellt und wird derzeit auf Ihrem Container-Service ausgeführt. Der Container-Service kann jeweils nur über eine Bereitstellung verfügen.
- Inaktiv – Ihre zuvor erfolgreich erstellte Bereitstellung wird nicht mehr auf Ihrem Container ausgeführt.
- Fehlgeschlagen — Ihre Bereitstellung ist fehlgeschlagen, da ein oder mehrere der in der Bereitstellung angegebenen Container nicht gestartet werden konnten.

Voraussetzungen

Bevor Sie beginnen, müssen Sie einen Lightsail-Container-Services erstellen. Weitere Informationen finden Sie unter Erstellen eines Container-Services.

Sie sollten auch eine Bereitstellung in Ihrem Container-Service erstellen, mit der Ihre Container konfiguriert und gestartet werden. Weitere Informationen finden Sie unter Erstellen und Verwalten von Bereitstellungen für Ihre Amazon Lightsail-Container-Services.

Anzeigen der Bereitstellungsversionen eines Container-Services

Führen Sie das folgende Verfahren aus, um die Containerprotokolle Ihres Lightsail-Container-Services anzuzeigen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen des Container-Services aus, für den Sie die Bereitstellungsversionen anzeigen möchten.
4. Wählen Sie die Registerkarte Images auf der Verwaltungsseite Ihres Container-Services aus.

   Die Bereitstellungen listet ggf. Ihre aktuellen Bereitstellungs- und Bereitstellungsversionen auf.
5. Die Bereitstellungsversionen Ihres Container-Services sind unter dem Abschnitt Bereitstellungsversionen der Seite aufgelistet.

   Jede Bereitstellung verfügt über ein Datum, an dem sie erstellt wurde, einen Status und ein Aktionsmenü.
6. Wählen Sie im Menü Aktionen einer Bereitstellungsversion eine der folgenden Optionen aus:

   - Eine neue Bereitstellung auswählen – Wählen Sie diese Option, um eine neue Bereitstellung aus der ausgewählten Bereitstellungsversion zu erstellen. Weitere Informationen zum Erstellen einer Bereitstellung finden Sie unter Erstellen oder Ändern der Container-Services-Bereitstellung.

     > **Note**
     >
     > Wenn Sie eine neue Bereitstellung mit Status Fehlgeschlagen aus einer Version erstellen möchten, müssen Sie die Ursache des Fehlers korrigieren, bevor Sie die Bereitstellung erstellen. Andernfalls schlägt die Bereitstellung wahrscheinlich erneut fehl.

   - View details (Details anzeigen) – Wählen Sie diese Option, um den Containereintrag und die öffentlichen Endpunktparameter der ausgewählten Bereitstellungsversion anzuzeigen. Sie können auch die Containerprotokolle für die Bereitstellung anzeigen, falls Sie eine fehlerhafte Bereitstellung diagnostizieren müssen. Weitere Informationen finden Sie unter Anzeigen von Container-Services-Protokollen.

Lightsail-Container-Serviceprotokolle anzeigen

Jeder Container in Ihrer Amazon Lightsail-Container-Service-Bereitstellung generiert ein Protokoll. Die Containerprotokolle stellen die stdout- und stderr-Streams von Prozessen bereit, die in Ihren Containern ausgeführt werden. Greifen Sie regelmäßig auf die Protokolle Ihrer Container zu, um deren Vorgänge zu diagnostizieren. Die letzten drei Tage der Protokolleinträge werden gespeichert, bevor die ältesten durch die neuesten Einträge ersetzt werden.

Filtern von Containerprotokollen

Containerprotokolle können Hunderte von Einträgen pro Tag haben. Verwenden Sie die Filteroptionen, um die Anzahl der Einträge zu reduzieren, die im Protokollfenster angezeigt werden, und erleichtern Sie die Suche nach dem, was Sie suchen. Sie können Containerprotokolle nach einem Start- und Enddatum (in Ortszeit) und nach einem bestimmten Begriff filtern. Beim Filtern nach einem Term können Sie Protokolleinträge für den angegebenen Begriff ein- oder ausschließen.

Der Filterbegriff Einschließen oder Ausschließen sucht nach einer genauen Übereinstimmung, bei der die Groß-/Kleinschreibung beachtet wird. Wenn Sie z. B. angeben, dass nur Protokollereignisse eingeschlossen werden sollen, die `HTTP` in der Nachricht haben, dann sehen Sie alle Protokollereignisse, die `HTTP` in der Nachricht beinhalten, aber keine, die `http` in der Nachricht beinhalten. Wenn Sie angeben, dass `Error` ausgeschlossen werden soll, dann werden Sie alle Protokollereignisse, die nicht `Error` in der Nachricht beinhalten und auch Protokollereignisse, die `ERROR` in der Mitteilung beinhalten, sehen.

Voraussetzungen

Bevor Sie beginnen, müssen Sie einen Lightsail-Container-Services erstellen. Weitere Informationen finden Sie unter Erstellen von Amazon-Lightsail-Container-Services.

Sie sollten auch eine Bereitstellung in Ihrem Container-Service erstellen, mit der Ihre Container konfiguriert und gestartet werden. Weitere Informationen finden Sie unter Erstellen und Verwalten von Bereitstellungen für Ihre Amazon Lightsail-Container-Services.

Anzeigen von Containerprotokollen

Führen Sie das folgende Verfahren aus, um die Containerprotokolle Ihres Lightsail-Container-Services anzuzeigen.

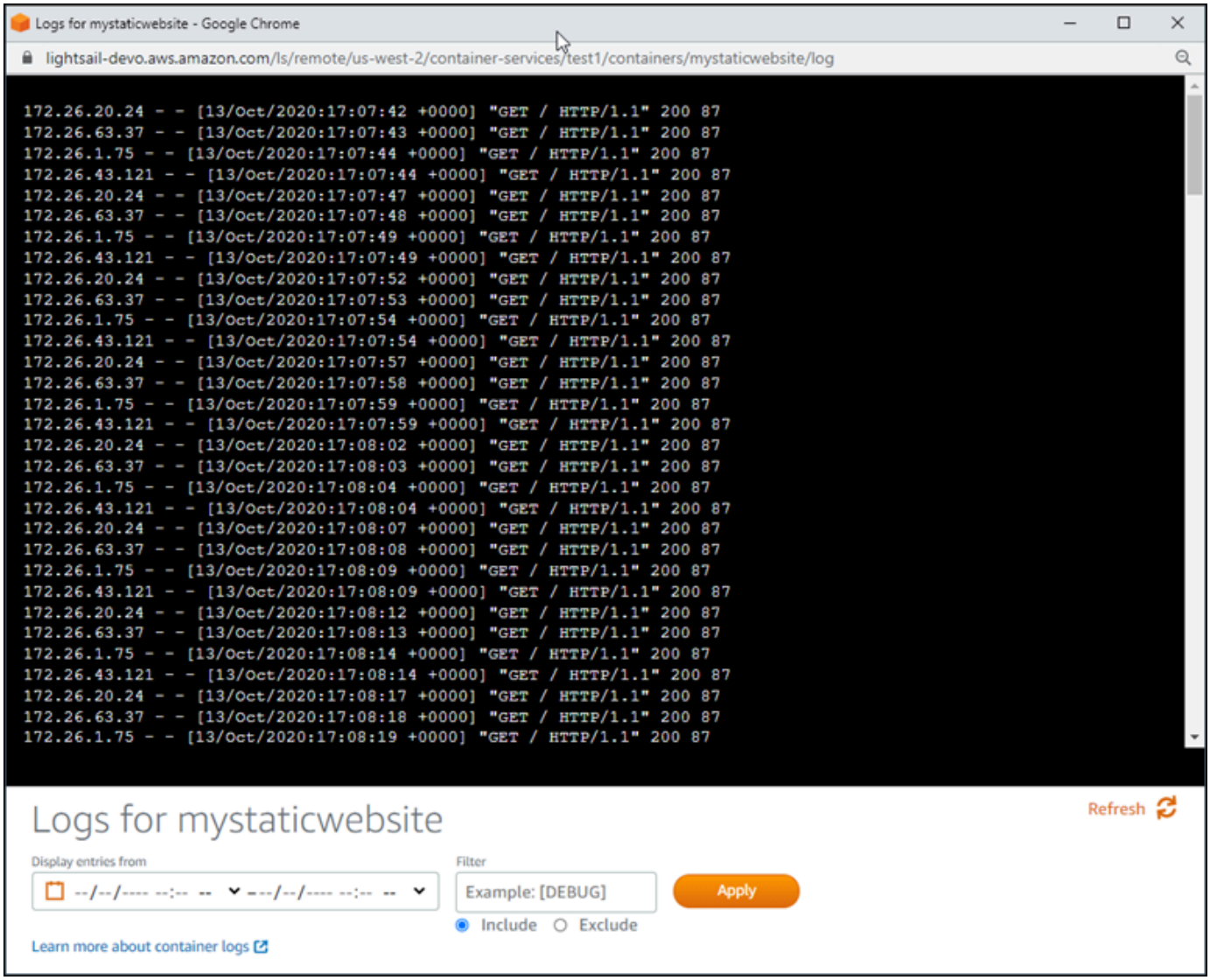
1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen des Container-Servicess aus, für den Sie die aktivierten benutzerdefinierten Domänen anzeigen möchten.
4. Wählen Sie die Registerkarte Images auf der Verwaltungsseite Ihres Container-Servicess aus.

   Die Seite Bereitstellungen listet ggf. Ihre aktuellen Bereitstellungen und Bereitstellungsversionen auf.
5. Wählen Sie eine der folgenden Optionen, um Containerprotokolle anzuzeigen:

   - Um auf die Containerprotokolle der aktuellen Bereitstellung zuzugreifen, wählen Sie Protokoll öffnen für die Containereinträge unter dem Abschnitt Aktuelle Bereitstellung der Seite.
   - Um auf die Containerprotokolle einer früheren Bereitstellung zuzugreifen, wählen Sie das Aktionsmenü-Symbol (⋮) für eine vorherige Bereitstellung unter dem Abschnitt Bereitstellungsversionen der Seite und wählen Sie Details anzeigen. In derDetails zur Versiondie Option Protokoll öffnen für die aufgelisteten Containereinträge aus.

   Das Containerprotokoll wird in einem neuen Browser-Fenster geöffnet. Sie können nach unten scrollen, um weitere Protokolleinträge anzuzeigen, und die Seite aktualisieren, um die neuesten Einträge zu laden. Die Filteroptionen werden unten auf der Seite angezeigt.

   > **Note**
   >
   > Protokolleinträge werden in aufsteigender Reihenfolge und in koordinierter Weltzeit (Coordinated Universal Time, UTC) angezeigt. Das heißt, die ältesten Protokolleinträge befinden sich oben und Sie müssen nach unten scrollen, um neuere Protokolleinträge anzuzeigen.



Aktivieren und verwalten Sie benutzerdefinierte Domains in Lightsail

Aktivieren Sie benutzerdefinierte Domains für Ihren Amazon Lightsail-Containerservice, um Ihre registrierten Domainnamen mit Ihrem Service zu verwenden. Bevor Sie benutzerdefinierte Domänen aktivieren, akzeptiert Ihr Container-Service Datenverkehr nur für die Standarddomäne, die Ihrem Dienst zugeordnet ist, wenn Sie ihn zum ersten Mal erstellen (z. B.`containerservicename.123456abcdef.us-west-2.cs.amazonlightsail.com`) enthalten. Wenn Sie benutzerdefinierte Domänen aktivieren, wählen Sie das Lightsail-SSL-/TLS-Zertifikat aus, das Sie für die Domänen erstellt haben, die Sie mit Ihrem Container-Service

verwenden möchten, und wählen Sie dann die Domänen aus, die Sie von diesem Zertifikat verwenden möchten. Nachdem Sie benutzerdefinierte Domänen aktiviert haben, akzeptiert der Container-Service Datenverkehr für alle Domänen, die dem ausgewählten Zertifikat zugeordnet sind.

> **Important**
>
> Wenn Sie einen Lightsail-Containerservice als Ursprung Ihrer Verteilung auswählen, fügt Lightsail automatisch den Standard Domainnamen Ihrer Verteilung als benutzerdefinierte Domain zu Ihrem Containerservice hinzu. Auf diese Weise kann der Datenverkehr zwischen Ihrer Verteilung und Ihrem Containerservice geleitet werden. Es gibt jedoch einige Umstände, unter denen Sie möglicherweise den Standard Domainnamen Ihrer Verteilung manuell zu Ihrem Containerservice hinzufügen müssen. Weitere Informationen finden Sie unter Hinzufügen der Standard-Domain einer Verteilung zu einem Container-Service.

Inhalt

Benutzerdefinierte Domäneneinschränkungen für den Container-Service

Die folgenden Einschränkungen gelten für benutzerdefinierte Domänen für Container-Services:

- Sie können bis zu 4 benutzerdefinierte Domänen mit jedem Ihrer Lightsail-Container-Services verwenden und Sie können dieselben Domänen nicht für mehr als einem Dienst verwenden.
- Wenn Sie eine Lightsail-DNS-Zone verwenden, um das DNS Ihrer Domäne zu verwalten, können Sie Datenverkehr für die Spitze Ihrer Domäne (z. B. `example.com`) und für Unterdomänen (z. B. `www.example.com`) zu Ihren Container-Services weiterleiten.

Voraussetzungen

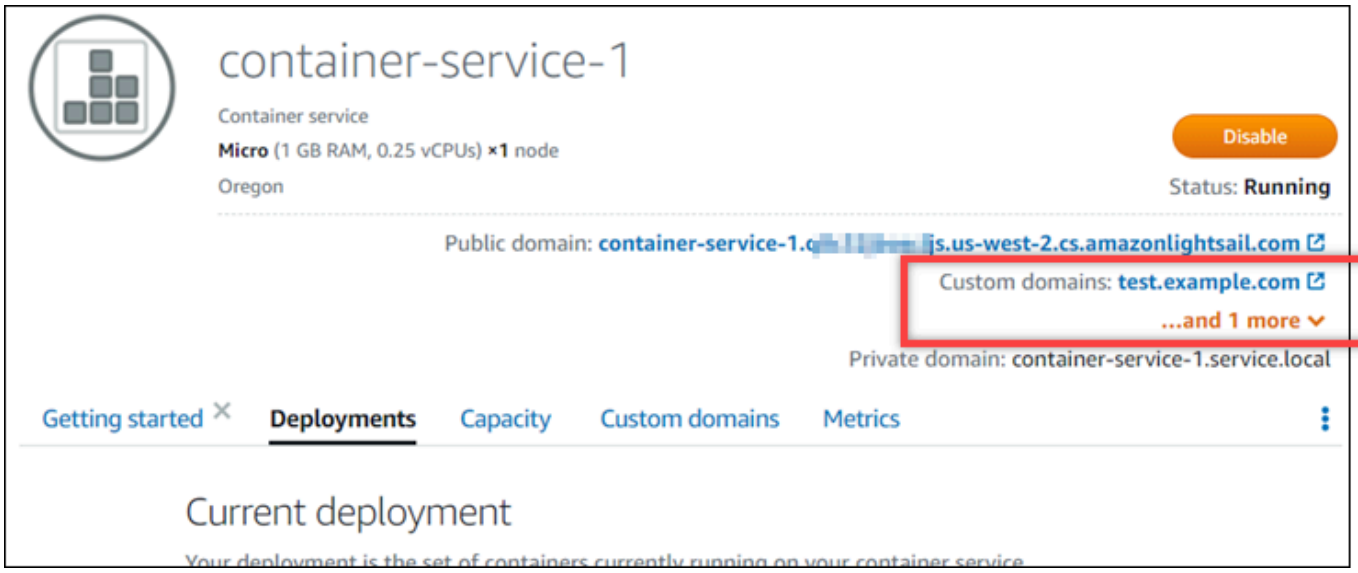
Bevor Sie beginnen, müssen Sie einen Lightsail-Container-Services erstellen. Weitere Informationen finden Sie unter Erstellen von Amazon Lightsail-Container-Services.

Außerdem sollten Sie ein SSL-/TLS-Zertifikat für Ihren Container-Service erstellt und validiert haben. Weitere Informationen finden Sie unter SSL/TLS-Zertifikate für Container-Services erstellen und SSL/TLS-Zertifikate für Container-Services validieren.

Anzeigen benutzerdefinierter Domänen für einen Container-Service

Vervollständigen Sie das folgende Verfahren, um die benutzerdefinierten Domänen anzuzeigen, die derzeit für Ihren Container-Service aktiviert sind.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen des Container-Servicess aus, für den Sie die aktivierten benutzerdefinierten Domänen anzeigen möchten.
4. Finden Sie die benutzerdefinierten Domänenwerte in der Überschrift der Container-Service-Verwaltungsseite, wie in folgendem Beispiel dargestellt. Dies sind die benutzerdefinierten Domänen, die derzeit für den Container-Service aktiviert sind.



5. Wählen Sie die Registerkarte Benutzerdefinierte Domänen auf der Verwaltungsseite Ihres Container-Servicess aus.

Die benutzerdefinierten Domänen, die unter jedem angefügten Zertifikat verwendet werden, sind unter dem Abschnitt Benutzerdefinierte Domänen-SSL-/TLS-Zertifikate der Seite aufgelistet. Die Zertifikate, die derzeit Ihrem Container-Service angefügt sind, sind im Abschnitt Attached certificates (Angefügte Zertifikate) aufgeführt.

Aktivieren benutzerdefinierter Domänen für einen Container-Service

Vervollständigen Sie das folgende Verfahren, um benutzerdefinierte Domänen für Ihren Lightsail-Container-Service zu aktivieren, indem Sie ein Zertifikat an Ihren Dienst anfügen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen des Container-Servicess aus, für den Sie benutzerdefinierte Domänen aktivieren möchten.
4. Wählen Sie die Registerkarte Benutzerdefinierte Domänen auf der Verwaltungsseite Ihres Container-Servicess aus.

   Die Seite Benutzerdefinierte Domänen stellt die SSL-/TLS-Zertifikate dar, die derzeit Ihrem Container-Service angefügt sind, falls vorhanden.
5. Wählen Sie Anfügen eines Zertifikatsaus.

   Wenn Sie keine Zertifikate haben, müssen Sie zunächst ein SSL-/TLS-Zertifikat für Ihre Domains erstellen und dann validieren, bevor Sie es an Ihren Container-Service anfügen können. Weitere Informationen finden Sie unter Erstellen von SSL-/TLS-Zertifikaten für Container-Services.
6. Wählen Sie im daraufhin angezeigten Dropdown-Menü ein gültiges Zertifikat für die Domäne(n) aus, die Sie mit Ihrem Container-Service verwenden möchten.
7. Vergewissern Sie sich, dass die Zertifikatsinformationen korrekt sind, und wählen Sie dann Attach (Anfügen) aus.
8. Der Status des Containerdienstes ändert sich in Updating (Wird aktualisiert). Nachdem der Status in Ready (Bereit) geändert wurde, wird die Domäne des Zertifikats im Abschnitt Custom domains (Benutzerdefinierte Domänen) angezeigt.
9. Wählen Sie Add domain assignment (Domainzuweisung hinzufügen) aus, um die Domain auf Ihren Container-Service zu verweisen.

10. Vergewissern Sie sich, dass das Zertifikat und die DNS-Informationen korrekt sind, und wählen Sie dann Add assignment (Zuweisung hinzufügen). Nach einigen Augenblicken wird der Datenverkehr für die von Ihnen ausgewählte Domäne von Ihrem Container-Service akzeptiert.
11. Nachdem Sie die Domänenzuweisung hinzugefügt haben, öffnen Sie ein neues Browserfenster und navigieren Sie zu der benutzerdefinierten Domäne, die Sie für den Container-Service aktiviert haben. Die Anwendung, die auf Ihrem Container-Service ausgeführt wird, falls vorhanden, sollte geladen werden.

Deaktivieren benutzerdefinierter Domänen für einen Container-Service

Vervollständigen Sie das folgende Verfahren, um benutzerdefinierte Domänen für Ihren Lightsail-Container-Service zu deaktivieren, indem Sie ein Zertifikat von Ihrem Dienst trennen oder eine zuvor ausgewählte Domäne deaktivieren.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen des Container-Servicess aus, für den Sie benutzerdefinierte Domänen deaktivieren möchten.
4. Wählen Sie die Registerkarte Benutzerdefinierte Domänen auf der Verwaltungsseite Ihres Container-Servicess aus.

   Die Seite Benutzerdefinierte Domänen stellt die SSL-/TLS-Zertifikate dar, die derzeit Ihrem Container-Service angefügt sind, falls vorhanden.
5. Wählen Sie eine der folgenden Optionen:

   1. Wählen Sie Configure container service domains (Konfigurieren von Container-Service-Domänen) aus, um entweder Domänen abzuwählen, die zuvor ausgewählt wurden, oder um weitere Domänen auszuwählen, die dem Container-Service zugeordnet sind.
   2. Wählen Sie Trennen aus, um das Zertifikat vom Container-Service zu trennen und alle zugehörigen Domains vom Service zu entfernen.

> **Important**
>
> Wenn Sie dies noch nicht getan haben, ändern Sie die DNS-Akten Ihrer Domäne so, dass Datenverkehrs-Routen das Routing zu Ihrem Container-Service stoppen und stattdessen an eine andere Ressource weiterleiten.

Themen

Weiterleiten von Datenverkehr für eine Domain zu einem Lightsail-Container-Service

Sie müssen Ihren registrierten Domainnamen an Ihren Amazon Lightsail-Container-Service verweisen, nachdem Sie die benutzerdefinierte Domain für Ihren Dienst aktiviert haben. Um dies zu tun, fügen Sie der DNS-Zone jeder Domäne einen Alias-Datensatz hinzu, die in den Zertifikaten, die Sie mit Ihrem Container-Service verwenden, angegeben sind. Alle Akten, die Sie hinzufügen, sollten auf die Standarddomäne (z. B.`https://<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`) Ihres Container-Servicess verweisen.

In diesem Leitfaden stellen wir Ihnen das Verfahren zur Verfügung, mit dem Sie Ihre Domain mithilfe einer Lightsail-DNS-Zone auf Ihren Container-Service verweisen können. Weitere Informationen über Lightsail DNS-Zonen finden Sie unter DNS in Amazon Lightsail.

Weitere Informationen zu Container-Services finden Sie unter Container-Services.

> **Note**
>
> Wenn Sie Route 53 verwenden, um den DNS Ihrer Domain zu hosten, sollten Sie den Alias-Datensatz der gehosteten Zone Ihrer Domain in Route 53 hinzufügen. Weitere Informationen finden Sie unter Weiterleiten von Datenverkehr für eine Domain in Route 53 zu einem Amazon Lightsail-Container-Service.

Voraussetzung

Bevor Sie beginnen, sollten Sie benutzerdefinierte Domains für Ihren Lightsail-Container-Service aktivieren. Weitere Informationen finden Sie unter Aktivieren und Verwalten benutzerdefinierter Domänen für Ihre Amazon Lightsail-Container-Services.

Abrufen der Standarddomäne Ihres Container-Servicess

Führen Sie das folgende Verfahren aus, um den Standard-Domänennamen Ihres Container-Servicess abzurufen, den Sie beim Hinzufügen einem Alias-Datensatz zum DNS Ihrer Domäne angeben.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.
3. Wählen Sie den Namen eines Container-Servicess, für den der Standarddomänenname abgerufen werden soll.
4. Notieren Sie sich im Kopfbereich Ihrer Container-Serviceverwaltungsseite Ihren Standarddomänennamen. Ihr Standarddomänenname des Container-Servicess ist ähnlich wie`<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`.

   Sie müssen diesen Wert als Teil einer Canonical-Name-Akte (CNAME) im DNS Ihrer Domänen hinzufügen. Es wird empfohlen, diesen Wert in eine Textdatei zu kopieren und einzufügen, auf die Sie später verweisen können. Weitere Informationen finden Sie unter den folgenden Abschnitten Hinzufügen der CNAME-Akten zur DNS-Zone Ihrer Domäne in diesem Leitfaden.

Hinzufügen von Akten zur DNS-Zone Ihrer Domäne

Führen Sie das folgende Verfahren aus, um einen Adressenakte (A für IPv4 oder AAAA für IPv6) oder eine kanonische Akte (CNAME) zur DNS-Zone Ihrer Domäne hinzuzufügen.

1. Wählen Sie auf der Lightsail-Startseite die Registerkarte Domains & DNS (Domänen und DNS).
2. Wählen Sie unter dem Abschnitt DNS-Zonen der Seite den Domänennamen aus, zu dem Sie die Akte hinzufügen möchten, der den Datenverkehr für Ihre Domäne an Ihren Container-Service weiterleitet.
3. Wählen Sie die Registerkarte DNS records (DNS-Datensätze) aus.
4. Führen Sie je nach dem aktuellen Status Ihrer DNS-Zone einen der folgenden Schritte aus:

- Wenn Sie noch keinen A-, AAAA- oder CNAME-Datensatz hinzugefügt haben, wählen Sie Datensatz hinzufügen aus.
- Wenn Sie zuvor eine A-, AAAA- oder CNAME-Akte hinzugefügt haben, wählen Sie das Bearbeitungssymbol neben der vorhandenen A-, AAAA- oder CNAME-Akte aus, das auf der Seite aufgeführt ist, und fahren Sie dann mit Schritt 5 dieses Verfahrens fort.

5. Wählen Sie A-Akte, AAAA-Akte oder CNAME-Akte im Aktentyp Dropdown-Menü.

   - Fügen Sie eine A-Akte hinzu, um die Spitze Ihrer Domäne (z. B.`example.com`) oder eine Unterdomäne (z. B.`www.example.com`) an Ihren Container-Service im IPv4-Netzwerk zuzuordnen.
   - Fügen Sie eine AAAA-Akte hinzu, um die Spitze Ihrer Domäne (z. B.`example.com`) oder eine Unterdomäne (z. B.`www.example.com`) an Ihren Container-Service im IPv6-Netzwerk zuzuordnen.
   - Fügen Sie eine CNAME-Akte hinzu, um eine Unterdomäne (z. B. `www.example.com`) an die öffentliche Domäne (Standard-DNS) Ihres Container-Servicess zuzuordnen.

6. Geben Sie im Textfeld Record name (Datensatzname) eine der folgenden Optionen ein:

   - Geben Sie für eine A-Akte oder eine AAAA-Akte `@` ein, um den Datenverkehr für die Spitze Ihrer Domäne (z. B.`example.com`) an Ihren Container-Service weiterzuleiten oder geben Sie eine Unterdomäne ein (z. B.`www`), um den Datenverkehr für eine Unterdomäne (z. B.`www.example.com`) an Ihren Container-Service weiterzuleiten.
   - Geben Sie für eine CNAME-Akte eine Unterdomäne ein (z. B.`www`), um den Datenverkehr für eine Unterdonäne (z. B.`www.example.com`) an Ihren Container-Service weiterzuleiten.

7. Führen Sie einen der folgenden Schritte aus, je nachdem, welche Akte Sie hinzugefügt haben:

   - Wählen Sie für eine A-Akte oder eine AAAA-Akte den Namen Ihres Container-Servicess im TextfeldAuflösung in .
   - Geben Sie für eine CNAME-Akte den Standarddomänennamen Ihres Container-Servicess in das TextfeldZuordnung zu.

8. Wählen Sie das Symbol „Speichern“, um die Akte in Ihrer DNS-Zone zu speichern.

   Wiederholen Sie diese Schritte, um zusätzliche DNS-Akten für Domänen in Ihrem Zertifikat hinzuzufügen, das Sie mit dem Container-Service verwenden. Warten Sie einige Zeit, damit sich Änderungen über das DNS im Internet ausbreiten. Nach einigen Minuten sollten Sie sehen, ob Ihre Domäne auf Ihren Container-Service verweist.

Weiterleiten von Datenverkehr für eine Domain in Route 53 zu einem Lightsail-Container-Service

Sie können den Datenverkehr für eine registrierte Domäne, z. B. `example.com`, an die Anwendungen weiterleiten, die auf einem Lightsail-Container-Service ausgeführt werden. Dazu fügen Sie der gehosteten Zone Ihrer Domain einen Alias-Eintrag hinzu, der auf die Standarddomäne Ihres Lightsail-Container-Services verweist.

In diesem Tutorial zeigen wir Ihnen, wie Sie einen Alias-Eintrag für Ihren Lightsail-Container-Service zu einer gehosteten Zone in Route 53 hinzufügen. Diese Aufgabe können Sie nur mit der AWS Command Line Interface (AWS CLI) ausführen. Mit der Route-53-Konsole ist dies nicht möglich.

> **Note**
>
> Wenn Sie Lightsail verwenden, um den DNS Ihrer Domain zu hosten, dann sollten Sie den Alias-Datensatz der DNS-Zone Ihrer Domain in Lightsail hinzufügen. Weitere Informationen finden Sie unter Weiterleiten von Datenverkehr für eine Domäne in Amazon Lightsail zu einem Lightsail-Container-Service.

Inhalt

Schritt 1: Erfüllen der Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies noch nicht geschehen ist:

- Registrieren Sie einen Domainnamen in Route 53, oder machen Sie Route 53 zum DNS-Service für Ihren registrierten (vorhandenen) Domainnamen. Weitere Informationen finden Sie unter Domainnamen mit Amazon Route 53 registrieren oder Amazon Route 53 zum DNS-Service für eine vorhandene Domain machen im Entwicklerhandbuch für Amazon Route 53.
- Stellen Sie Ihre Anwendungen in Ihrem Lightsail-Container-Service bereit. Weitere Informationen finden Sie unter Erstellen und Verwalten von Bereitstellungen für Container-Services.

- Aktivieren Sie Ihren registrierten Domänennamen in Ihrem Lightsail-Container-Service. Weitere Informationen finden Sie unter Aktivieren und verwalten benutzerdefinierter Domains.
- Konfigurieren der AWS CLI mit Ihrem Konto. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

Schritt 2: Abrufen der ID der gehosteten Zone für Lightsail-Container-Services

Sie müssen eine ID der gehosteten Zone für Ihren Lightsail-Container-Service angeben, wenn Sie einer gehosteten Zone in Route 53 einen Alias-Datensatz hinzufügen. Wenn sich Ihr Lightsail-Container-Service beispielsweise in der AWS-Region USA West (Oregon) (us-west-2) befindet, müssen Sie die ID der gehosteten Zonen `Z0959753D43BBB908BAV` angeben, wenn Sie einen Alias-Datensatz für Ihren Lightsail-Container-Service zu einer gehosteten Zone in Route 53 hinzufügen.

Im Folgenden sind die gehosteten Zonen-IDs für jede AWS-Region aufgeführt, in der Sie einen Lightsail-Container-Service erstellen können.

Europa (London): (eu-west-2): Z0624918ZXDYQZLOXA66

USA Ost (Nord-Virginia): (us-east-1): Z06246771KYU0IRHI74W4

Asien-Pazifik (Singapur) (ap-southeast-1): Z0625921354DRJH4EY9V0

Europa (Irland) (eu-west-1): Z0624732FELAMMKW3Y21

Asien-Pazifik (Tokio) (ap-northeast-1): Z0626125UAU4JWQ9JSKN

Asien-Pazifik (Seoul) (ap-northeast-2): Z06260262XZM84B2WPLHH

Asien-Pazifik (Mumbai): (ap-south-1): Z10460781IQMISS0I0VVY

Asien-Pazifik (Sydney) (ap-southeast-2): Z09597943PQQZATPFE96E

Kanada (Zentral): (ca-central-1): Z10450993RIRIJJUUMA5W

Europa (Frankfurt): (eu-central-1): Z06137433FV04OY4EC6L0

Europa (Stockholm) (eu-north-1): Z016970523TDG2TZMUXKK

Europa (Paris): (eu-west-3): Z09594631DSW2QUR7CFGO

USA Ost (Ohio) (us-east-2): Z10362273VJ548563IY84

USA West (Oregon): (us-west-2): Z0959753D43BBB908BAV

Schritt 3: Erstellen einer JSON-Datei mit Datensatz

Wenn Sie der gehosteten Zone Ihrer Domain in Route 53 mithilfe der AWS CLI einen DNS-Eintrag hinzufügen, müssen Sie eine Reihe von Konfigurationsparametern für den Eintrag angeben. Der einfachste Weg, dies zu tun, besteht darin, eine JSON-Datei (.json) zu erstellen, die alle Parameter enthält, und dann in Ihrer AWS CLI-Anforderung auf die JSON-Datei zu verweisen.

Führen Sie das folgende Verfahren aus, um eine JSON-Datei mit den Datensatzparametern für den Aliasdatensatz zu erstellen:

1. Öffnen Sie einen Texteditor, z. B. Notepad unter Windows oder Nano unter Linux.
2. Kopieren Sie den folgenden Text und fügen Sie ihn in den Texteditor ein:

```
{
  "Comment": "Comment",
  "Changes": [
    {
      "Action": "CREATE",
      "ResourceRecordSet": {
        "Name": "Domain.",
        "Type": "A",
        "AliasTarget": {
          "HostedZoneId": "LightsailContainerServiceHostedZoneID",
          "DNSName": " LightsailContainerServiceAddress.",
          "EvaluateTargetHealth": true
        }
      }
    }
  ]
}
```

   Ersetzen Sie in Ihrer Datei den folgenden Beispieltext durch Ihren eigenen:

   - *Kommentar* mit einer persönlichen Notiz oder einem Kommentar zum Datensatzsatz.
   - *Domäne* mit dem registrierten Domänennamen, den Sie mit Ihrem Lightsail-Container-Service verwenden möchten (z. B. `example.com` oder `www.example.com`). Um das Stammverzeichnis Ihrer Domäne mit Ihrem Lightsail-Container-Service zu verwenden, müssen Sie ein @-Symbol im Subdomänenraum Ihrer Domäne angeben (z. B. `@.example.com`).
   - *LightsailContainerServiceHostedZoneID* mit der ID der gehosteten Zone für die AWS-Region, in der Sie Ihren Lightsail-Container-Service erstellt haben. Weitere

Informationen finden Sie weiter oben in diesem Leitfaden unter Schritt 2: Abrufen der gehosteten Zonen-IDs für Lightsail-Container-Services.

- *LightsailContainerServiceAddress* mit dem öffentlichen Domainnamen Ihres Lightsail-Container-Services. Sie können dies abrufen, indem Sie sich bei der Lightsail-Konsole anmelden, zu Ihrem Container-Service navigieren und die öffentliche Domäne kopieren, die im Kopfbereich der Verwaltungsseite des Container-Services aufgeführt ist (z. B. `container-service-1.q8cexampleljs.us-west-2.cs.amazonlightsail.com`).

Beispiel:

```
{
  "Comment": "Alias record for Lightsail container service",
  "Changes": [
    {
      "Action": "CREATE",
      "ResourceRecordSet": {
        "Name": "@.example.com.",
        "Type": "A",
        "AliasTarget": {
          "HostedZoneId": "Z0959753D43BBB908BAV",
          "DNSName": "container-service-1.q8cexampleljs.us-
west-2.cs.amazonlightsail.com.",
          "EvaluateTargetHealth": true
        }
      }
    }
  ]
}
```

3. Speichern Sie die Datei in Ihrem lokalen Verzeichnis als `change-resource-record-sets.json`.

Schritt 4: Hinzufügen eines Datensatzes zur gehosteten Zone Ihrer Domain in Route 53

Führen Sie das folgende Verfahren aus, um der gehosteten Zone Ihrer Domain in Route 53 mithilfe der AWS CLI einen Datensatz hinzuzufügen. Führen Sie dazu den `change-resource-record-sets`-Befehl aus. Weitere Informationen finden Sie unter change-resource-record-sets in der AWS CLI-Befehlsreferenz.

> **Note**
>
> Sie müssen die AWS CLI installieren und für Lightsail und Route 53 konfigurieren, bevor Sie mit diesem Vorgang fortfahren. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein, um einen Datensatz zur gehosteten Zone Ihrer Domäne in Route 53 hinzuzufügen.

```
aws route53 change-resource-record-sets --hosted-zone-id HostedZoneID --change-batch PathToJsonFile
```

Ersetzen Sie im Befehl den folgenden Beispieltext mit Ihrem eigenen:

- *HostedZoneID* mit der ID der gehosteten Zone für Ihre registrierte Domain in Route 53. Verwenden Sie den Befehl list-hosted-zones, um eine Liste der IDs für die gehosteten Zonen in Ihrem Route-53-Konto abzurufen.
- *PathToJsonFile* mit dem lokalen Verzeichnispfad auf Ihrem Computer der .json-Datei, die die Datensatzparameter enthält. Weitere Informationen finden Sie im Abschnitt Schritt 3: Erstellen einer Datensatzgruppen-JSON-Datei weiter oben in diesem Leitfaden.

Beispiele:

Auf einem Linux- oder Unix-Computer:

```
aws route53 change-resource-record-sets --hosted-zone-id Z123456789ABCDEFGHIJ --change-batch home/user/awscli/route53/change-resource-record-sets.json
```

Auf einem Windows-Computer:

```
aws route53 change-resource-record-sets --hosted-zone-id Z123456789ABCDEFGHIJ --change-batch file://C:\awscli\route53\change-resource-record-sets.json
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

```
H:\>aws route53 change-resource-record-sets --hosted-zone-id Z123456789ABCDEFGHIJ
--change-batch file://C:\awscli\route53\change-resource-record-sets.json
                    -
{
    "ChangeInfo": {
        "Id": "/change/C05953EXAMPLEZ4V4LOAC",
        "Status": "PENDING",
        "SubmittedAt": "2021-08-11T20:58:30.960000+00:00",
        "Comment": "Alias record for Lightsail container service"
    }
}
```

Lassen Sie der Änderung Zeit, sich über das DNS des Internets zu verbreiten, was mehrere Stunden dauern kann. Nachdem dies abgeschlossen ist, sollte der Internetverkehr für Ihre registrierte Domain in Route 53 mit der Weiterleitung an Ihren Lightsail-Container-Service beginnen.

Sicherheit in Amazon Lightsail

Die Sicherheit in der Cloud hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit gilt zwischen AWS und Ihnen eine geteilte Verantwortung. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS-Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Weitere Informationen zu den Compliance-Programmen und den Services, für die sie gelten, finden Sie unter Im Rahmen des Compliance-Programms zugelassene AWS-Services.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung von Amazon Lightsail einsetzen können. Die folgenden Themen veranschaulichen, wie Sie Amazon Lightsail zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie erfahren auch, wie Sie andere AWS-Services nutzen können, die Ihnen bei der Überwachung und Sicherung Ihrer Amazon Lightsail-Ressourcen helfen.

Sicherheit der Infrastruktur in Amazon Lightsail

Als verwalteter Service ist Amazon Lightsail durch die globalen Verfahren zur Gewährleistung der Netzwerksicherheit von AWS geschützt. Informationen zu AWS-Sicherheitsservices und wie AWS die Infrastruktur schützt, finden Sie unter AWS-Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Lightsail zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.

- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Ausfallsicherheit in Amazon Lightsail

Die globale AWS-Infrastruktur ist um AWS-Regionen und Availability Zones herum aufgebaut. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die mit einem Netzwerk mit geringer Latenz, hohem Durchsatz und hoher Redundanz verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen über AWS-Regionen und Availability Zones finden Sie unter AWSGlobale Infrastruktur.

Zusätzlich zur globalen AWS-Infrastruktur stellt Amazon Lightsail verschiedene Funktionen bereit, um Ihren Anforderungen in Bezug auf Ausfallsicherheit und Datensicherung zu erfüllen.

- Kopieren von Instance- und Datenträger-Snapshots über Regionen hinweg. Weitere Informationen finden Sie unter Snapshots.
- Automatisieren von Snapshots von Instance- und Datenträger-Snapshots. Weitere Informationen finden Sie unter Snapshots.
- Verteilung des eingehenden Datenverkehrs auf mehrere Instances in einer einzigen Availability Zone oder mehreren Availability Zones mit einem Load Balancer. Weitere Informationen finden Sie unter Load Balancer.

Identity and Access Management für Amazon Lightsail

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in Amazon Lightsail.

Service user (Service-Benutzer) – Wenn Sie den Amazon Lightsail-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere Amazon Lightsail-Funktionen ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Featuresweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie auf ein Feature in Amazon Lightsail keinen Zugriff haben, finden Sie unter Fehlerbehebung von Identity and Access Management (IAM) weitere Informationen.

Service administrator (Service-Administrator) – Wenn Sie in Ihrem Unternehmen für Amazon Lightsail-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Amazon Lightsail. Ihre Aufgabe besteht darin, die Amazon Lightsail-Funktionen und -Ressourcen festzulegen, auf die Mitarbeiter zugreifen können sollten. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Amazon Lightsail verwenden kann, finden Sie unter So funktioniert Amazon Lightsail mit IAM.

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Amazon Lightsail verfassen können. Zum Anzeigen von beispielhaften identitätsbasierten Amazon Lightsail-Richtlinien, die Sie in IAM verwenden können, finden Sie unter Beispiele für identitätsbasierte Amazon Lightsail-Richtlinien.

Authentifizierung mit Identitäten

Die Authentifizierung ist die Art und Weise, wie Sie sich mit Ihren Anmeldeinformationen bei AWS anmelden. Weitere Informationen zur Anmeldung über die AWS Management Console finden Sie unter Die IAM-Konsole und Anmeldeseite im IAM-Benutzerhandbuch.

Sie müssen als AWS-Konto-Stammbenutzer oder als IAM-Benutzer authentifiziert (bei AWS angemeldet) sein oder eine IAM-Rolle annehmen. Sie können auch die Single-Sign-on-

Authentifizierung Ihres Unternehmens verwenden oder sich sogar über Google oder Facebook anmelden. In diesen Fällen hat Ihr Administrator vorher einen Identitätsverbund unter Verwendung von IAM-Rollen eingerichtet. Wenn Sie mit Anmeldeinformationen eines anderen Unternehmens auf AWS zugreifen, nehmen Sie indirekt eine Rolle an.

Um sich direkt bei der AWS Management Console anzumelden, verwenden Sie Ihr Passwort mit der E-Mail Ihres Stammbenutzers oder den Namen Ihres IAM-Benutzers. Sie können auf AWS programmgesteuert oder mit Ihren Stamm- oder IAM-Benutzerzugriffsschlüsseln zugreifen. AWS stellt SDK- und Befehlszeilen-Tools bereit, mit denen Ihre Anforderung anhand Ihrer Anmeldeinformationen kryptografisch signiert wird. Wenn Sie keine AWS-Tools verwenden, müssen Sie die Anforderung selbst signieren. Hierzu verwenden Sie Signature Version 4, ein Protokoll für die Authentifizierung eingehender API-Anforderungen. Weitere Informationen zur Authentifizierung von Anfragen finden Sie unter Signature Version 4-Signaturprozess im Allgemeine AWS-Referenz.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise auch zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise die Verwendung von Multi-Factor Authentication (MFA), um die Sicherheit Ihres Kontos zu verbessern. Weitere Informationen finden Sie unter Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-KontoAWS-Konto-Root-Benutzer

Wenn Sie ein AWS-Konto neu erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen des Kontos hat. Diese Identität wird als AWS-Konto-Root-Benutzer bezeichnet. Für den Zugriff auf den Root-Benutzer müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder eine einzelne Anwendung. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen

wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität in Ihrem AWS-Konto mit spezifischen Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der AWS Management Console übernehmen, indem Sie Rollen wechseln. Sie können eine Rolle annehmen, indem Sie eine AWS CLI oder AWS-API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center-Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.

- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff – Einige AWS-Services verwenden Features in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in Amazon Managed Service for Prometheus verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anforderungen werden nur dann gestellt, wenn ein Dienst eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden zu können. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Serviceverknüpfte Rolle – Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen in Amazon EC2 – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen,

als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil, das an die Instance angefügt ist, um eine AWS-Rolle einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center-Benutzerhandbuch.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff – Einige AWS-Services verwenden Features in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Service

kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.

- Prinzipalberechtigungen – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Richtlinien gewähren einem Prinzipal Berechtigungen. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Informationen dazu, ob eine Aktion zusätzliche abhängige Aktionen in einer Richtlinie erfordert, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lightsail in der Service-Autorisierungs-Referenz.
- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Serviceverknüpfte Rolle – Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen in Amazon EC2 – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil, das an die Instance angefügt ist, um eine AWS-Rolle einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Für die Zugriffssteuerung in AWS erstellen Sie Richtlinien und weisen diese den AWS-Identitäten oder -Ressourcen zu. Eine Richtlinie ist ein Objekt in AWS, das, wenn es einer Identität oder

Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Benutzerinformationen über die AWS Management Console, die AWS CLI oder die AWS -API abrufen.

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Eine IAM-Entität (Benutzer oder Rolle) besitzt zunächst keine Berechtigungen. Anders ausgedrückt, können Benutzer standardmäßig keine Aktionen ausführen und nicht einmal ihr Passwort ändern. Um einem Benutzer die Berechtigung für eine Aktion zu erteilen, muss ein Administrator einem Benutzer eine Berechtigungsrichtlinie zuweisen. Alternativ kann der Administrator den Benutzer zu einer Gruppe hinzufügen, die über die gewünschten Berechtigungen verfügt. Wenn ein Administrator einer Gruppe Berechtigungen erteilt, erhalten alle Benutzer in dieser Gruppe diese Berechtigungen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Benutzerinformationen über die AWS Management Console, die AWS CLI oder die AWS -API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem AWS-Konto anfügen können. Verwaltete Richtlinien umfassen von AWS verwaltete und von Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können verwaltete AWS-Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und

Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3, AWS WAF und Amazon VPC sind Beispiele für Dienste, die ACLs unterstützen. Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Ein ausdrückliches Ablehnen in einer dieser Richtlinien setzt das Zulassen außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OE) in AWS Organizations

angeben. AWS Organizations ist ein Dienst für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. SCPs schränken Berechtigungen für Entitäten in Mitgliedskonten einschließlich des jeweiligen Root-Benutzer des AWS-Kontos ein. Weitere Informationen zu Organisationen und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations-Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die resultierenden Berechtigungen sind eine Schnittmenge der identitätsbasierten Richtlinien der Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Ein ausdrückliches Ablehnen in einer dieser Richtlinien setzt das Zulassen außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OE) in AWS Organizations angeben. AWS Organizations ist ein Dienst für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Funktionen aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Eine SCP beschränkt die Berechtigungen für Entitäten in Mitgliedskonten, einschließlich aller AWS-Konto-Stammbenutzer. Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations-Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie

stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS die Zulässigkeit einer Anforderung ermittelt, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik für die Richtlinienauswertung im IAM-Benutzerhandbuch.

Themen

- AWS Von verwaltete Richtlinien für Amazon Lightsail
- Funktionsweise von Amazon Lightsail mit IAM
- Verwalten von Zugriff auf Amazon Lightsail für IAM-Benutzer

AWS Von verwaltete Richtlinien für Amazon Lightsail

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, von AWS verwaltete Richtlinien zu verwenden, als selbst Richtlinien zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere von AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu verwalteten AWS-Richtlinien finden Sie unter Verwaltete AWS-Richtlinien im IAM-Leitfaden.

AWS-Services pflegen und Aktualisieren von verwalteten AWS-Richtlinien. Die Berechtigungen in von AWS verwalteten Richtlinien können nicht geändert werden. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Services entfernen keine Berechtigungen aus einer von AWS verwalteten Richtlinie, so dass Richtlinien-Aktualisierungen Ihre vorhandenen Berechtigungen nicht beeinträchtigen.

Darüber hinaus unterstützt AWS verwaltete Richtlinien für Auftragsfunktionen, die mehrere Services umfassen. Die von ReadOnlyAccessAWS verwaltete Richtlinie bietet beispielsweise

schreibgeschützten Zugriff auf alle AWS-Services und -Ressourcen. Wenn ein Service ein neues Feature startet, fügt AWS schreibgeschützte Berechtigungen für neue Vorgänge und Ressourcen hinzu. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS-Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

AWS-verwaltete Richtlinie: LightsailExportAccess

Sie können LightsailExportAccess nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die Lightsail die Durchführung von Aktionen in Ihrem Namen ermöglicht. Weitere Informationen finden Sie unter Serviceverknüpfte Rollen.

Diese Richtlinie gewährt Berechtigungen, die es Lightsail ermöglichen, Ihre Instance- und Festplatten-Snapshots nach Amazon Elastic Compute Cloud zu exportieren und die aktuelle Konfiguration „Blockieren des öffentlichen Zugriffs“ auf Kontoebene von Amazon Simple Storage Service (Amazon S3) abzurufen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `ec2` – Ermöglicht den Zugriff zum Auflisten und Kopieren von Instance-Images und Festplatten-Snapshots.
- `iam` – Ermöglicht den Zugriff auf das Löschen von serviceverknüpften Rollen und das Abrufen des Status des Löschens Ihrer serviceverknüpften Rollen.
- `s3` – Ermöglicht den Zugriff zum Abrufen der `PublicAccessBlock`-Konfiguration für ein AWS-Konto.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iam:DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
   ],
   "Resource": "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
  },
```

```
  {
   "Effect": "Allow",
   "Action": [
    "ec2:CopySnapshot",
    "ec2:DescribeSnapshots",
    "ec2:CopyImage",
    "ec2:DescribeImages"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "s3:GetAccountPublicAccessBlock"
   ],
   "Resource": "*"
  }
 ]
}
```

Lightsail-Aktualisierungen für AWS verwaltete Richtlinien

- Bearbeiten der von `LightsailExportAccess` verwaltete Richtlinie

  Die `s3:GetAccountPublicAccessBlock`-Aktion wurde der von `LightsailExportAccess` verwalteten Richtlinie hinzugefügt. Dies ermöglicht Lightsail, die aktuelle Konfiguration „Blockieren des öffentlichen Zugriffs“ auf Kontoebene von Amazon S3 abzurufen.

  14. Januar 2022
- Lightsail hat die Änderungsverfolgung gestartet

  Lightsail hat mit der Verfolgung von Änderungen für seine AWS-verwalteten Richtlinien begonnen.

  14. Januar 2022

Funktionsweise von Amazon Lightsail mit IAM

Bevor Sie IAM zum Verwalten des Zugriffs auf Lightsail verwenden, sollten Sie wissen, welche IAM-Funktionen für die Verwendung mit Lightsail verfügbar sind. Einen Überblick über das Zusammenwirken von Lightsail und anderen AWS-Services mit IAM finden Sie unter AWS-Services, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Identitätsbasierte Lightsail-Richtlinien

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Lightsail unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Aktionen

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Richtlinienaktionen in Lightsail verwenden das folgende Präfix vor der Aktion: `lightsail:`. Um einem Benutzer beispielsweise die Berechtigung zum Ausführen einer Lightsail-Instance mit der Lightsail-API-Operation `CreateInstances` zu erteilen, fügen Sie die Aktion `lightsail:CreateInstances` in die entsprechende Richtlinie ein. Richtlinienanweisungen müssen entweder ein `Action`- oder ein `NotAction`-Element enthalten. Lightsail definiert eine eigene Gruppe von Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service durchführen können.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt durch Kommata:

```
"Action": [
      "lightsail:action1",
      "lightsail:action2"
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Create` beginnen, einschließlich der folgenden Aktion:

```
"Action": "lightsail:Create*"
```

Eine Liste der Lightsail-Aktionen finden Sie im IAM-Benutzerhandbuch unter Aktionen, die von Amazon Lightsaildefiniert werden.

Ressourcen

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource`- oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

> **Important**
>
> Lightsail unterstützt keine Berechtigungen auf Ressourcenebene für einige API-Aktionen. Weitere Informationen finden Sie unter Unterstützung für Berechtigungen auf Ressourcenebene und Autorisierung auf der Basis von Tags.

Die Lightsail-Instance-Ressource hat den folgenden ARN:

```
arn:${Partition}:lightsail:${Region}:${Account}:Instance/${InstanceId}
```

Weitere Informationen zum Format von ARNs finden Sie unter Amazon-Ressourcennamen (ARNs) und AWS-Service-Namespaces.

Wenn Sie beispielsweise die `ea123456-e6b9-4f1d-b518-3ad1234567e6`-Instance in Ihrer Anweisung angeben möchten, verwenden Sie den folgenden ARN:

```
"Resource": "arn:aws:lightsail:us-east-1:123456789012:Instance/ea123456-e6b9-4f1d-
b518-3ad1234567e6"
```

Um alle Instances anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (*):

```
"Resource": "arn:aws:lightsail:us-east-1:123456789012:Instance/*"
```

Einige Lightsail-Aktionen, z. B. zum Erstellen von Ressourcen, können auf bestimmten Ressourcen nicht ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (*) verwenden.

```
"Resource": "*"
```

Viele Lightsail-API-Aktionen umfassen mehrere Ressourcen. Beispiel: `AttachDisk` hängt einen Lightsail-Blockspeicherdatenträger an eine Instance an, damit ein IAM-Benutzer Berechtigungen für die Verwendung des Datenträgers und der Instance haben muss. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie die ARNs durch Kommata voneinander.

```
"Resource": [
      "resource1",
      "resource2"
```

Eine Liste der Lightsail-Ressourcentypen und ihrer ARNs finden Sie unter Von Amazon Lightsail definierte Ressourcen im IAM-Benutzerhandbuch. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von Amazon Lightsail definierte Aktionen.

Bedingungsschlüssel

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte

Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mittels einer logischen OR-Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Lightsail stellt keine servicespezifischen Bedingungsschlüssel bereit, unterstützt jedoch die Verwendung einiger globaler Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste der Lightsail-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon Lightsail im IAM-Benutzerhandbuch. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon Lightsail definierte Aktionen.

Beispiele

Beispiele für identitätsbasierte Lightsail-Richtlinien finden Sie unter Beispiele für identitätsbasierte Amazon Lightsail-Richtlinien.

Ressourcenbasierte Lightsail-Richtlinien

Lightsail unterstützt keine ressourcenbasierten Richtlinien.

Zugriffskontrolllisten (ACLs)

Lightsail bietet keine Unterstützung für Zugriffskontrolllisten (Access Control Lists, ACLs).

Autorisierung auf der Basis von Lightsail-Tags

Sie können Tags an Lightsail-Ressourcen anfügen oder Tags in einer Anforderung an Lightsail übergeben. Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `lightsail:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder `aws:TagKeys`Bedingung verwenden.

> **Important**
>
> Lightsail unterstützt keine Autorisierung auf Basis von Tags für einige API-Aktionen. Weitere Informationen finden Sie unter Unterstützung für Berechtigungen auf Ressourcenebene und Autorisierung auf der Basis von Tags.

Weitere Informationen zum Tagging von Lightsail-Ressourcen finden Sie unter Tags.

Ein Beispiel für eine identitätsbasierte Richtlinie zum Einschränken des Zugriffs auf eine Ressource auf der Basis der Tags dieser Ressource finden Sie unter Erstellen und Löschen von Lightsail-Ressourcen auf der Basis von Tags erlauben.

IAM-Rollen für Lightsail

Eine IAM-Rolle ist eine Entität in Ihrem AWS-Konto mit spezifischen Berechtigungen.

Verwenden temporärer Anmeldeinformationen mit Lightsail

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Temporäre Sicherheitsanmeldeinformationen erhalten Sie durch Aufrufen von AWS STS-API-Vorgängen wie AssumeRole oder GetFederationToken.

Lightsail unterstützt die Verwendung temporärer Anmeldeinformationen.

Serviceverknüpfte Rollen

Serviceverknüpfte Rollen erlauben AWS-Services den Zugriff auf Ressourcen in anderen Services, um eine Aktion in Ihrem Auftrag auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Lightsail unterstützt serviceverknüpfte Rollen. Weitere Informationen zum Erstellen oder Verwalten von serviceverknüpften Lightsail-Rollen finden Sie unter Verwenden von serviceverknüpften Rollen.

Servicerollen

Lightsail unterstützt keine Servicerollen.

Themen

- Amazon LightsailBeispiele für identitätsbasierte -Richtlinien
- Amazon Lightsail-Richtlinienbeispiele auf Ressourcenebene
- Verwenden von serviceverknüpften Rollen für Amazon Lightsail
- IAM-Richtlinie zum Verwalten von Buckets in Amazon Lightsail

Amazon LightsailBeispiele für identitätsbasierte -Richtlinien

IAM-Benutzer besitzen keine Berechtigungen zum Erstellen oder Ändern von Lightsail-Ressourcen. Sie können auch keine Aufgaben ausführen, die die AWS Management Console-, AWS CLI- oder AWS-API benutzen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den IAM-Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Amazon Lightsail-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS-verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie die AWS-verwaltete Richtlinien die Berechtigungen für viele allgemeine Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto verfügbar. Wir empfehlen Ihnen, die

Berechtigungen weiter zu reduzieren, indem Sie AWS-kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien oder AWS-verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise AWS CloudFormation, verwendet werden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Bedarf einer Multi-Faktor-Authentifizierung (MFA) – Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Lightsail-Konsole

Für den Zugriff auf die Amazon Lightsail-Konsole benötigen Sie Vollzugriffsberechtigungen für alle Lightsail-Aktionen und -Ressourcen. Diese Berechtigungen müssen Ihnen das Auflisten und Anzeigen von Details zu den Lightsail-Ressourcen in Ihrem AWS-Konto gestatten. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen (z. B ohne Vollzugriff), funktioniert die Konsole nicht wie vorgesehen für Entitäten (IAM-Benutzer oder -Rollen) mit dieser Richtlinie.

Um sicherzustellen, dass diese Entitäten dennoch die Lightsail-Konsole verwenden können, fügen Sie den Entitäten die folgende Richtlinie an. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Für Benutzer, die nur Aufrufe an die AWS CLI oder AWS-API durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die den API-Operation entsprechen, die Sie ausführen möchten.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie enthält Berechtigungen für die Ausführung dieser Aktion auf der Konsole oder für die programmgesteuerte Ausführung über die AWS CLI oder die AWS-API.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Zulassen von Erstellung und Löschung von Lightsail-Ressourcen basierend auf Tags

Sie können in Ihrer identitätsbasierten Richtlinie Bedingungen für die Steuerung des Zugriffs auf Lightsail-Ressourcen auf der Basis von Tags verwenden. In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen können, mit der Benutzer nur dann neue Lightsail-Ressourcen erstellen können, wenn ein Schlüsseltag von `allow` und ein Wert von `true` mit der Erstellungsanforderung definiert ist. Diese Richtlinie beschränkt außerdem das Löschen von Ressourcen, es sei denn, sie haben den Schlüssel-Wert-Tag `allow/true`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "lightsail:Create*",
                "lightsail:TagResource",
                "lightsail:UntagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/allow": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:Delete*",
                "lightsail:TagResource",
                "lightsail:UntagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/allow": "true"
                }
            }
        }
    ]
}
```

Das folgende Beispiel hindert Benutzer daran, das Tag für Ressourcen zu ändern, die ein anderes Schlüssel-Wert-Tag als `allow/false` haben.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "lightsail:TagResource"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "StringNotEquals": {
                    "aws:ResourceTag/allow": "false"
                }
            }
        }
    ]
}
```

Sie können diese Richtlinien den IAM-Benutzern in Ihrem Konto anhängen. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

Amazon Lightsail-Richtlinienbeispiele auf Ressourcenebene

Berechtigungen auf Ressourcenebene bedeutet, dass Sie angeben können, für welche Ressourcen die Benutzer Aktionen ausführen dürfen. Von Amazon Lightsail unterstützte Berechtigungen auf Ressourcenebene Das heißt, Sie können bei bestimmten Lightsail-Aktionen kontrollieren, wann die Benutzer diese Aktionen verwenden dürfen. Dies basiert auf Bedingungen, die erfüllt sein müssen, oder auf bestimmten Ressourcen, die von den Benutzern verwendet oder bearbeitet werden dürfen. Beispielsweise können Sie den Benutzern auch Berechtigungen zur Verwaltung einer Instance oder Datenbank mit einem bestimmten Amazon-Ressourcenname (ARN) erteilen.

> **Important**
>
> Lightsail unterstützt keine Berechtigungen auf Ressourcenebene für einige API-Aktionen. Weitere Informationen finden Sie unter Unterstützung für Berechtigungen auf Ressourcenebene und Autorisierung auf der Basis von Tags.

Weitere Informationen zu den Ressourcen, die durch die Lightsail-Aktionen erstellt oder geändert werden, sowie über die ARNs und Lightsail-Bedingungsschlüssel, die Sie in einer IAM-Richtlinienerklärung verwenden können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lightsail im IAM-Benutzerhandbuch.

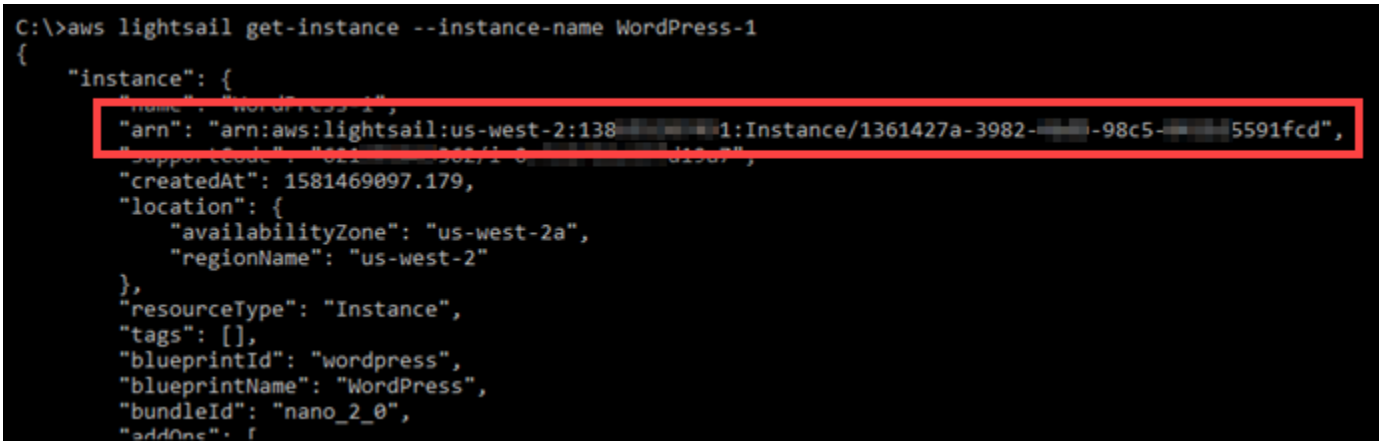
Zulassen der Verwaltung einer bestimmten Instance

Die folgende Richtlinie gewährt den Zugriff zum Neustarten/Starten/Stoppen einer Instance, zum Verwalten von Instance-Ports und zum Erstellen von Instance-Snapshots für eine bestimmte Instance. Sie bietet auch schreibgeschützten Zugriff auf andere Instance-bezogene Informationen und Ressourcen im Lightsail-Konto. Ersetzen Sie in der Richtlinie *`InstancEarn`* durch den Amazon-Ressourcenname (ARN) Ihrer Instance.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "lightsail:GetActiveNames",
                "lightsail:GetAlarms",
                "lightsail:GetAutoSnapshots",
                "lightsail:GetBlueprints",
                "lightsail:GetBundles",
                "lightsail:GetCertificates",
                "lightsail:GetCloudFormationStackRecords",
                "lightsail:GetContactMethods",
                "lightsail:GetDisk",
                "lightsail:GetDisks",
                "lightsail:GetDiskSnapshot",
                "lightsail:GetDiskSnapshots",
                "lightsail:GetDistributionBundles",
                "lightsail:GetDistributionLatestCacheReset",
                "lightsail:GetDistributionMetricData",
                "lightsail:GetDistributions",
                "lightsail:GetDomain",
                "lightsail:GetDomains",
                "lightsail:GetExportSnapshotRecords",
                "lightsail:GetInstance",
                "lightsail:GetInstanceAccessDetails",
                "lightsail:GetInstanceMetricData",
                "lightsail:GetInstancePortStates",
                "lightsail:GetInstances",
                "lightsail:GetInstanceSnapshot",
                "lightsail:GetInstanceSnapshots",
                "lightsail:GetInstanceState",
                "lightsail:GetKeyPair",
                "lightsail:GetKeyPairs",
                "lightsail:GetLoadBalancer",
                "lightsail:GetLoadBalancerMetricData",
                "lightsail:GetLoadBalancers",
                "lightsail:GetLoadBalancerTlsCertificates",
                "lightsail:GetOperation",
                "lightsail:GetOperations",
                "lightsail:GetOperationsForResource",
```

```
                "lightsail:GetRegions",
                "lightsail:GetRelationalDatabase",
                "lightsail:GetRelationalDatabaseBlueprints",
                "lightsail:GetRelationalDatabaseBundles",
                "lightsail:GetRelationalDatabaseEvents",
                "lightsail:GetRelationalDatabaseLogEvents",
                "lightsail:GetRelationalDatabaseLogStreams",
                "lightsail:GetRelationalDatabaseMetricData",
                "lightsail:GetRelationalDatabaseParameters",
                "lightsail:GetRelationalDatabases",
                "lightsail:GetRelationalDatabaseSnapshot",
                "lightsail:GetRelationalDatabaseSnapshots",
                "lightsail:GetStaticIp",
                "lightsail:GetStaticIps",
                "lightsail:IsVpcPeered"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "lightsail:CloseInstancePublicPorts",
                "lightsail:CreateInstanceSnapshot",
                "lightsail:OpenInstancePublicPorts",
                "lightsail:PutInstancePublicPorts",
                "lightsail:RebootInstance",
                "lightsail:StartInstance",
                "lightsail:StopInstance"
            ],
            "Resource": "InstanceARN"
        }
    ]
}
```

Um den ARN für Ihre Instance abzurufen, verwenden Sie die Lightsail-API-Aktion `GetInstance` und geben Sie den Namen der Instance mithilfe des `instanceName`-Parameters an. Ihr Instance-ARN wird in den Ergebnissen dieser Aktion aufgeführt, wie im folgenden Beispiel gezeigt. Weitere Informationen finden Sie unter GetInstance in der Amazon Lightsail-API-Referenz.



Zulassen der Verwaltung einer bestimmten Datenbank

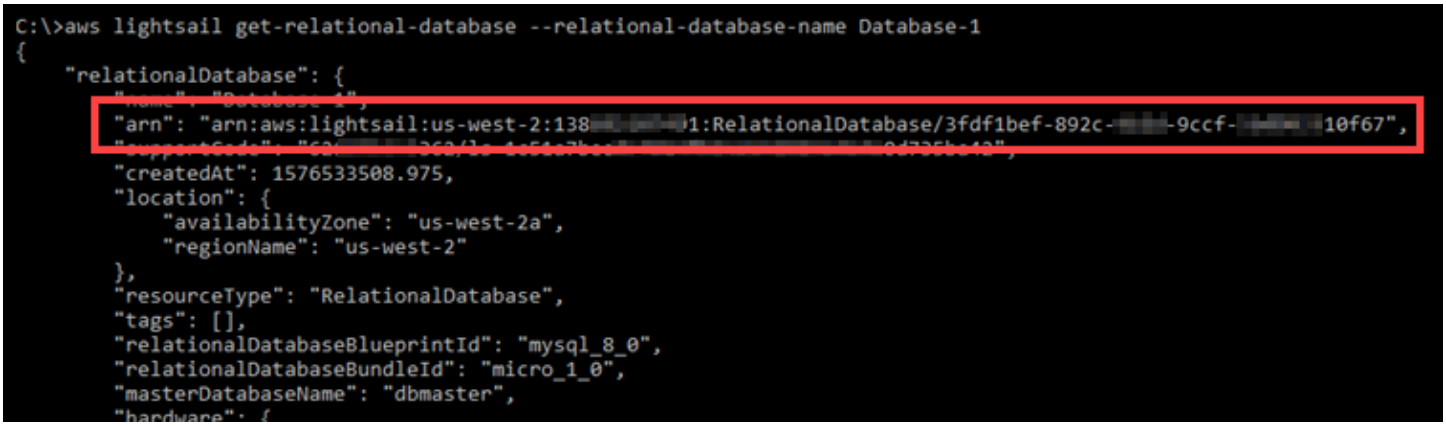
Die folgende Richtlinie gewährt Zugriff auf die Aktionen Neustarten/Starten/Stoppen und Aktualisieren einer bestimmten Datenbank. Sie bietet auch schreibgeschützten Zugriff auf andere datenbankbezogene Informationen und Ressourcen im Lightsail-Konto. Ersetzen Sie in der Richtlinie *DatabasEarn* durch den Amazon-Ressourcenname (ARN) Ihrer Datenbank.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "lightsail:GetActiveNames",
                "lightsail:GetAlarms",
                "lightsail:GetAutoSnapshots",
                "lightsail:GetBlueprints",
                "lightsail:GetBundles",
                "lightsail:GetCertificates",
                "lightsail:GetCloudFormationStackRecords",
                "lightsail:GetContactMethods",
                "lightsail:GetDisk",
                "lightsail:GetDisks",
                "lightsail:GetDiskSnapshot",
                "lightsail:GetDiskSnapshots",
                "lightsail:GetDistributionBundles",
                "lightsail:GetDistributionLatestCacheReset",
                "lightsail:GetDistributionMetricData",
                "lightsail:GetDistributions",
                "lightsail:GetDomain",
```

```
                "lightsail:GetDomains",
                "lightsail:GetExportSnapshotRecords",
                "lightsail:GetInstance",
                "lightsail:GetInstanceAccessDetails",
                "lightsail:GetInstanceMetricData",
                "lightsail:GetInstancePortStates",
                "lightsail:GetInstances",
                "lightsail:GetInstanceSnapshot",
                "lightsail:GetInstanceSnapshots",
                "lightsail:GetInstanceState",
                "lightsail:GetKeyPair",
                "lightsail:GetKeyPairs",
                "lightsail:GetLoadBalancer",
                "lightsail:GetLoadBalancerMetricData",
                "lightsail:GetLoadBalancers",
                "lightsail:GetLoadBalancerTlsCertificates",
                "lightsail:GetOperation",
                "lightsail:GetOperations",
                "lightsail:GetOperationsForResource",
                "lightsail:GetRegions",
                "lightsail:GetRelationalDatabase",
                "lightsail:GetRelationalDatabaseBlueprints",
                "lightsail:GetRelationalDatabaseBundles",
                "lightsail:GetRelationalDatabaseEvents",
                "lightsail:GetRelationalDatabaseLogEvents",
                "lightsail:GetRelationalDatabaseLogStreams",
                "lightsail:GetRelationalDatabaseMetricData",
                "lightsail:GetRelationalDatabaseParameters",
                "lightsail:GetRelationalDatabases",
                "lightsail:GetRelationalDatabaseSnapshot",
                "lightsail:GetRelationalDatabaseSnapshots",
                "lightsail:GetStaticIp",
                "lightsail:GetStaticIps",
                "lightsail:IsVpcPeered"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "lightsail:RebootRelationalDatabase",
                "lightsail:StartRelationalDatabase",
                "lightsail:StopRelationalDatabase",
```

```
                "lightsail:UpdateRelationalDatabase"
            ],
            "Resource": "DatabaseARN"
        }
    ]
}
```

Um den ARN für Ihre Datenbank abzurufen, verwenden Sie die Lightsail-API-Aktion `GetRelationalDatabase` und geben Sie den Namen der Datenbank mit dem `relationalDatabaseName`-Parameter an. Ihr Datenbank-ARN wird in den Ergebnissen dieser Aktion aufgeführt, wie im folgenden Beispiel gezeigt. Weitere Informationen finden Sie unter GetRelationalDatabase in der Amazon Lightsail-API-Referenz.



Verwenden von serviceverknüpften Rollen für Amazon Lightsail

Amazon Lightsail verwendet serviceverknüpfte Rollen von AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit Amazon Lightsail verknüpft ist. Serviceverknüpfte Rollen werden von Amazon Lightsail vordefiniert und umfassen alle Berechtigungen, die Lightsail zum Aufrufen anderer AWS-Services in Ihrem Namen benötigt.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von Amazon Lightsail, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon Lightsail definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur Amazon Lightsail die Rollen übernehmen. Die definierten Berechtigungen enthält die Vertrauens- und Berechtigungsrichtlinie, die keinen anderen IAM-Entitäten zugewiesen werden kann.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre Amazon Lightsail-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für Amazon Lightsail

Amazon Lightsail verwendet die serviceverknüpfte Rolle AWSServiceRoleForLightsail – Rolle, um Lightsail-Instance- und Blockspeicher-Festplatten-Snapshots nach Amazon Elastic Compute Cloud (Amazon EC2) zu exportieren und die aktuelle Block-Public-Access-Konfiguration auf Kontoebene von Amazon Simple Storage Service (Amazon S3) abzurufen.

Die serviceverknüpfte Rolle AWSServiceRoleForLightsail vertraut den folgenden Services, die diese Rolle annehmen:

- `lightsail.amazonaws.com`

Die Rollenberechtigungsrichtlinie erlaubt Amazon Lightsail die Durchführung der folgenden Aktionen für die angegebenen Ressourcen:

- Aktion: `ec2:CopySnapshot` auf alle AWS-Ressourcen.
- Aktion: `ec2:DescribeSnapshots` auf alle AWS-Ressourcen.
- Aktion: `ec2:CopyImage` auf alle AWS-Ressourcen.
- Aktion: `ec2:DescribeImages` auf alle AWS-Ressourcen.
- Aktion: `cloudformation:DescribeStacks` auf alle AWS-AWS CloudFormation-Stacks.
- Aktion: `s3:GetAccountPublicAccessBlock` auf alle AWS-Ressourcen.

Berechtigungen von serviceverknüpften Rollen

Sie müssen Berechtigungen konfigurieren, damit eine IAM-Entität (z. B. Benutzer, Gruppen oder Rollen) die Beschreibung einer serviceverknüpften Rolle erstellen oder bearbeiten können.

So erlauben Sie einer IAM-Entität das Erstellen einer bestimmten serviceverknüpften Rolle

Fügen Sie die folgende Richtlinie der IAM-Entität hinzu, um die serviceverknüpfte Rolle zu erstellen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*",
            "Condition": {"StringLike": {"iam:AWSServiceName":
 "lightsail.amazonaws.com"}}
        },
        {
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
            "Resource": "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
        }
    ]
}
```

So erlauben Sie einer IAM-Entität das Erstellen einer beliebigen serviceverknüpften Rolle

Fügen Sie die folgende Anweisung der Berechtigungsrichtlinie für die IAM-Entität hinzu, um eine serviceverknüpfte Rolle oder eine beliebige Servicerolle zu erstellen, die die benötigten Richtlinien enthält. Diese Richtlinie fügt eine Richtlinie an die Rolle an.

```
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

So erlauben Sie einer IAM-Entität das Bearbeiten der Beschreibung von beliebigen Servicerollen

Fügen Sie die folgende Anweisung der Berechtigungsrichtlinie für die IAM-Entität hinzu, um die Beschreibung einer serviceverknüpften Rolle oder einer beliebigen Servicerolle zu bearbeiten.

```
{
```

```
    "Effect": "Allow",
    "Action": "iam:UpdateRoleDescription",
    "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

So erlauben Sie einer IAM-Entität das Löschen einer bestimmten serviceverknüpften Rolle

Fügen Sie die folgende Anweisung der Berechtigungsrichtlinie für die IAM-Entität hinzu, die die serviceverknüpfte Rolle löschen soll.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
}
```

So erlauben Sie einer IAM-Entität das Löschen einer beliebigen Servicerolle

Fügen Sie die folgende Anweisung der Berechtigungsrichtlinie für die IAM-Entität hinzu, die eine serviceverknüpfte Rolle oder eine beliebige Servicerolle löschen soll.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

Alternativ können Sie eine verwaltete AWS-Richtlinie verwenden, um Vollzugriff auf den Service zu gewähren.

Erstellen einer serviceverknüpften Rolle für Amazon Lightsail

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie Ihren Lightsail-Instance- oder Blockspeicher-Festplatten-Snapshot nach Amazon EC2 exportieren oder einen Lightsail-Bucket in der AWS AWS Management Console, der AWS CLI oder der AWS-API erstellen oder aktualisieren, wird von Amazon Lightsail die serviceverknüpfte Rolle für Sie erstellt.

Wenn Sie diese dienstverknüpfte Rolle löschen und erneut erstellen müssen, können Sie die Rolle in Ihrem Konto auf dieselbe Weise neu erstellen. Wenn Sie Ihren Lightsail-Instance- oder Blockspeicher-Festplatten-Snapshot nach Amazon EC2 exportieren oder einen Lightsail-Bucket erstellen oder aktualisieren, wird von Amazon Lightsail die serviceverknüpfte Rolle für Sie erstellt.

> **Important**
>
> Sie müssen die IAM-Berechtigungen so konfigurieren, dass es Amazon Lightsail erlaubt ist, die servicegebundene Rolle zu erstellen. Führen Sie dazu die Schritte aus, die sich im folgenden Abschnitt Berechtigungen von serviceverknüpften Rollen befinden.

Bearbeiten einer serviceverknüpften Rolle für Amazon Lightsail

Amazon Lightsail berechtigt Sie nicht zum Bearbeiten der serviceverknüpften Rolle AWSServiceRoleForCloudLightsail. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Amazon Lightsail

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch bestätigen, dass keine Amazon Lightsail-Instance- oder Festplatten-Snapshots in einem ausstehenden Kopierzustand vorhanden sind, bevor Sie die serviceverknüpfte Rolle AWSServiceRoleForLightsail löschen können. Weitere Informationen finden Sie unter Exportieren von Snapshots nach Amazon EC2.

So löschen Sie die servicegebundene Rolle mit IAM

Verwenden Sie die IAM-Konsole, die AWS CLI oder die AWS-API, um die serviceverknüpfte Rolle AWSServiceRoleForLightsail zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte Amazon Lightsail-Rollen

Amazon Lightsail unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen zu den Regionen, in denen Lightsail verfügbar ist, finden Sie unter Amazon Lightsail-Regionen.

IAM-Richtlinie zum Verwalten von Buckets in Amazon Lightsail

Die folgende Richtlinie gewährt einem Benutzer Zugriff auf die Verwaltung eines bestimmten Buckets im Amazon Lightsail-Objektspeicher-Service. Diese Richtlinie gewährt Zugriff auf Buckets mit der Lightsail-Konsole, der AWS Command Line Interface (AWS CLI), AWS-API und AWS-SDKs. Ersetzen Sie in der Richtlinie*<BucketName>* mit dem Namen des zu verwaltenden Buckets. Weitere Informationen zum Erstellen von IAM-Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im AWS Identity and Access Management-Benutzerhandbuch. Weitere Informationen zum Erstellen von IAM-Benutzern und -Benutzergruppen finden Sie unter Erstellen Ihres ersten delegierten IAM-Benutzers und Ihrer ersten IAM-Benutzergruppe im AWS Identity and Access Management-Benutzerhandbuch.

> **Important**
>
> Bei Benutzern ohne diese Richtlinie treten Fehler auf, wenn sie die Registerkarte Objekte der Bucket-Verwaltungsseite in der Lightsail-Konsole aufrufen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LightsailAccess",
            "Effect": "Allow",
            "Action": "lightsail:*",
            "Resource": "*"
        },
        {
            "Sid": "S3BucketAccess",
            "Effect": "Allow",
```

```
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::<BucketName>/*",
                "arn:aws:s3:::<BucketName>"
            ]
        }
    ]
}
```

Verwalten von Buckets und Objekten

Dies sind die allgemeinen Schritte zum Verwalten Ihres Lightsail-Objektspeicher-Buckets:

1. Weitere Informationen über Buckets und Objekte im Amazon Lightsail-Objektspeicherservice. Weitere Informationen zu Buckets finden Sie unter Objektspeicher in Amazon Lightsail.
2. Erfahren Sie mehr über die Namen, denen Sie Ihre Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Namensregeln für Buckets in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherservice, indem Sie ein Bucket erstellen. Weitere Informationen finden Sie unter Buckets erstellen in Amazon Lightsail.
4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Lightsail-Objektspeicher und Bucket-Berechtigungen in Amazon Lightsail verstehen.

   Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

   - Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail
   - Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail
   - Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
   - Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
   - Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail
   - Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail

5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherservice
   - Zugriffsprotokollierungsformat für Buckets im Amazon Lightsail-Objektspeicher-Service
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicher-Service
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail, um Anforderungen zu identifizieren
6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gewährt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets in Amazon Lightsail.
7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unterGrundlegendes zu Objektschlüsselnamen inAmazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Hochladen einer Datei in ein Bucket in Amazon Lightsail
   - Hochladen von Dateien in Buckets in Amazon Lightsail mit mehrteiligem Upload
   - Anzeigen von Objekten in einem Bucket in Amazon Lightsail
   - Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
   - Objekte von einem Bucket in Amazon Lightsail herunterladen
   - Filtern von Objekten in einem Bucket in Amazon Lightsail
   - Markieren von Objekten in einem Bucket in Amazon Lightsail
   - Löschen von Objekten in einem Bucket in Amazon Lightsail
9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.
10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.
11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.

12 Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrik-Alarmen in Amazon Lightsail.

13 Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Tarifs Ihres Buckets in Amazon Lightsail.

14 Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.

- Tutorial: Verbinden einer WordPress-Instance mit einem Amazon Lightsail-Bucket
- Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Lightsail-Netzwerkverteilung für die Bereitstellung von Inhalten

15 Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

Verwalten von Zugriff auf Amazon Lightsail für IAM-Benutzer

Als Root-Benutzer des AWS-Kontos oder AWS Identity and Access Management (IAM)-Benutzer mit Administratorzugriff können Sie einen oder mehrere IAM-Benutzer in Ihrem AWS-Konto erstellen, und diese Benutzer können mit unterschiedlichen Zugriffsebenen auf die von AWS angebotenen Services konfiguriert werden.

Für Amazon Lightsail möchten Sie vielleicht einen IAM-Benutzer anlegen, der nur auf den Lightsail-Service zugreifen kann. Sie können dies etwa machen, wenn jemand Ihrem Team beitritt, der Zugriff zum Anzeigen, Erstellen, Bearbeiten oder Löschen von Lightsail-Ressourcen benötigt, aber keinen Zugriff auf andere von AWS angebotene Dienste benötigt. Um dies zu konfigurieren, müssen Sie zunächst eine IAM-Richtlinie erstellen, die Zugriff auf Lightsail gewährt, dann erstellen Sie eine IAM-Gruppe und fügen die Richtlinie an die Gruppe an. Anschließend erstellen Sie IAM-Benutzer und machen sie zu Mitgliedern der Gruppe, die Zugriff auf Lightsail hat.

Wenn jemand Ihr Team verlässt, können Sie den Benutzer aus der Gruppe mit Zugriff auf Lightsail entfernen, um ihm den Zugang auf Lightsail wieder zu entziehen. Etwa dann, wenn jemand Ihr Team verlässt, jedoch weiterhin in Ihrem Unternehmen arbeitet. Alternativ können Sie den Benutzer auch aus IAM löschen, falls beispielsweise jemand Ihr Unternehmen verlässt und keinen Zugriff mehr benötigt.

Inhalt

- Erstellen einer IAM-Richtlinie für den Zugriff auf Lightsail
- Erstellen einer IAM-Gruppe für den Zugriff auf Lightsail und Hinzufügen der Lightsail-Zugriffsrichtlinie
- Erstellen eines IAM-Benutzers und Hinzufügen des Benutzers zur Lightsail-Zugriffsgruppe

Erstellen einer IAM-Richtlinie für den Zugriff auf Lightsail

Führen Sie die folgenden Schritte aus, um eine IAM-Richtlinie für den Zugriff auf Lightsail zu erstellen. Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien in der IAM-Dokumentation.

1. Melden Sie sich bei der IAM-Konsole an.
2. Wählen Sie im linken Navigationsbereich die Option Policies (Richtlinien) aus.
3. Wählen Sie Create Policy (Richtlinie erstellen) aus.
4. Wählen Sie auf der Seite Create Policy (Richtlinie erstellen) die Registerkarte JSON aus.

5. Markieren und kopieren Sie den Inhalt des Textfelds und fügen Sie ihn dann in den folgenden Konfigurationstext der Richtlinie ein.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:*"
            ],
            "Resource": "*"
        }
    ]
}
```

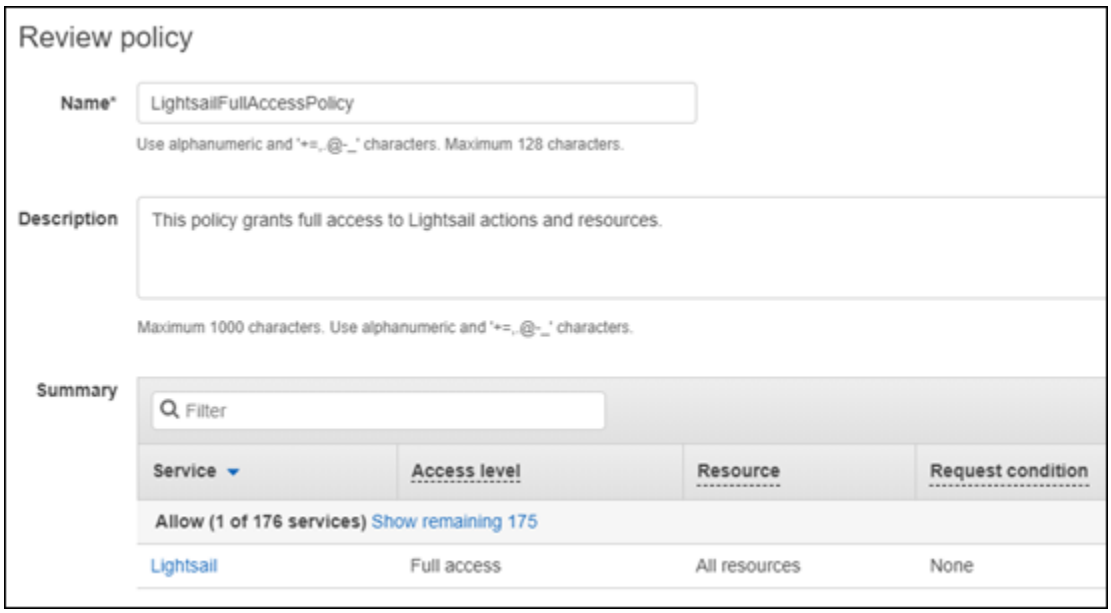
Das Ergebnis sollte wie folgt aussehen:

Dadurch gewähren Sie Zugriff auf alle Aktionen und Ressourcen von Lightsail. Aktionen, die den Zugriff auf andere von AWS angebotene Dienste erfordern, wie z.B. das Aktivieren von VPC-Peering, das Exportieren von Lightsail-Snapshots nach Amazon EC2 oder das Erstellen von Amazon EC2-Ressourcen mit Lightsail, erfordern zusätzliche Berechtigungen, die nicht in dieser Richtlinie enthalten sind. Weitere Informationen finden Sie in den folgenden Anleitungen:

- Einrichten von Amazon VPC-Peering-für die Zusammenarbeit mit AWS-Ressourcen außerhalb von Amazon Lightsail
- Exportieren von Amazon Lightsail-Snapshots nach Amazon EC2
- Erstellen von Amazon EC2-Instances aus exportierten Snapshots in Lightsail

Beispiele für Aktionsspezifische und ressourcenspezifische Berechtigungen, die Sie erteilen können, finden Sie unterAmazon LightsailBeispiele für Berechtigungsrichtilinien auf Ressourcenebene.

6. Wählen Sie Review policy (Richtlinie überprüfen) aus.
7. Benennen Sie auf der Seite Review Policy (Richtlinie überprüfen) die Richtlinie. Geben Sie einen aussagekräftigen Namen ein, z. B. `LightsailFullAccessPolicy`.
8. Fügen Sie eine Beschreibung hinzu und überprüfen Sie die Einstellungen der Richtlinie. Wenn Sie Änderungen vornehmen müssen, wählen Sie Previous (Zurück) um die Richtlinie zu ändern.



9. Wenn die Einstellungen der Richtlinie korrekt sind, wählen Sie Create Policy (Richtlinie erstellen).

   Die Richtlinie ist nun erstellt und kann zu einer bestehenden IAM-Gruppe hinzugefügt werden, oder Sie können eine neue IAM-Gruppe erstellen, indem Sie die Schritte im folgenden Abschnitt dieser Anleitung ausführen.

Erstellen einer IAM-Gruppe für den Zugriff auf Lightsail und Hinzufügen der Lightsail-Zugriffsrichtlinie

Führen Sie die folgenden Schritte aus, um eine IAM-Gruppe für den Zugriff auf Lightsail zu erstellen und um die Lightsail-Zugriffsrichtlinie aus dem vorherigen Abschnitt in dieser Anleitung hinzuzufügen. Weitere Informationen finden Sie unter Erstellen von IAM-Gruppen und Anfügen einer Richtlinie an eine IAM-Gruppe in der IAM-Dokumentation.

1. Wählen Sie im linken Navigationsbereich der IAM-Konsole die Option Gruppen.
2. Wählen Sie Create New Group (Neue Gruppe erstellen).
3. Benennen Sie die Gruppe auf der Seite Set Group Name (Gruppennamen festlegen). Geben Sie einen aussagekräftigen Namen ein, z. B. `LightsailFullAccessGroup`.
4. Suchen Sie auf der Seite Attach Policy (Richtlinie anfügen) die Lightsail-Richtlinie, die Sie zuvor in dieser Anleitung erstellt haben, z. B. `LightsailFullAccessPolicy`.
5. Fügen Sie ein Häkchen neben der Richtlinie hinzu und wählen Sie dann Next step (Weiter).
6. Überprüfen Sie die Einstellungen der Gruppe. Wenn Sie Änderungen vornehmen müssen, wählen Sie Previous (Zurück) um die Gruppenrichtlinie zu ändern.

7. Wenn die Einstellungen der Gruppe korrekt sind, wählen Sie Create Group (Gruppe erstellen).

   Die Gruppe ist jetzt erstellt, und Benutzer, die zur Gruppe hinzugefügt werden, haben nun Zugriff auf die Lightsail-Aktionen und -Ressourcen. Sie können vorhandene IAM-Benutzer zur Gruppe hinzufügen oder Sie können neue IAM-Benutzer erstellen, indem Sie die Schritte im folgenden Abschnitt dieser Anleitung befolgen.

Erstellen eines IAM-Benutzers und Hinzufügen des Benutzers zur Lightsail-Zugriffsgruppe

Führen Sie die folgenden Schritte aus, um einen IAM-Benutzer zu erstellen und um ihn zur Gruppe mit Zugriff auf Lightsail hinzuzufügen. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers in Ihrem AWS-Konto und Hinzufügen und Entfernen von Benutzern in einer IAM-Gruppe in der IAM-Dokumentation.

1. Wählen Sie im linken Navigationsbereich der IAM-Konsole die Option Benutzer.
2. Wählen Sie Benutzer hinzufügen.
3. Geben Sie im Bereich Set user details (Benutzerdetails festlegen) den Namen des Benutzers ein.
4. Wählen Sie im Abschnitt AWS-Zugriffstyp wählen auf der Seite eine der folgenden Optionen aus:

   a. Wählen Sie Programmatic Access (Programmzugriff), um eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel für die AWS API, CLI, SDK und anderen Entwicklungstools zu aktivieren, die für Lightsail-Aktionen und -Ressourcen verwendet werden können. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

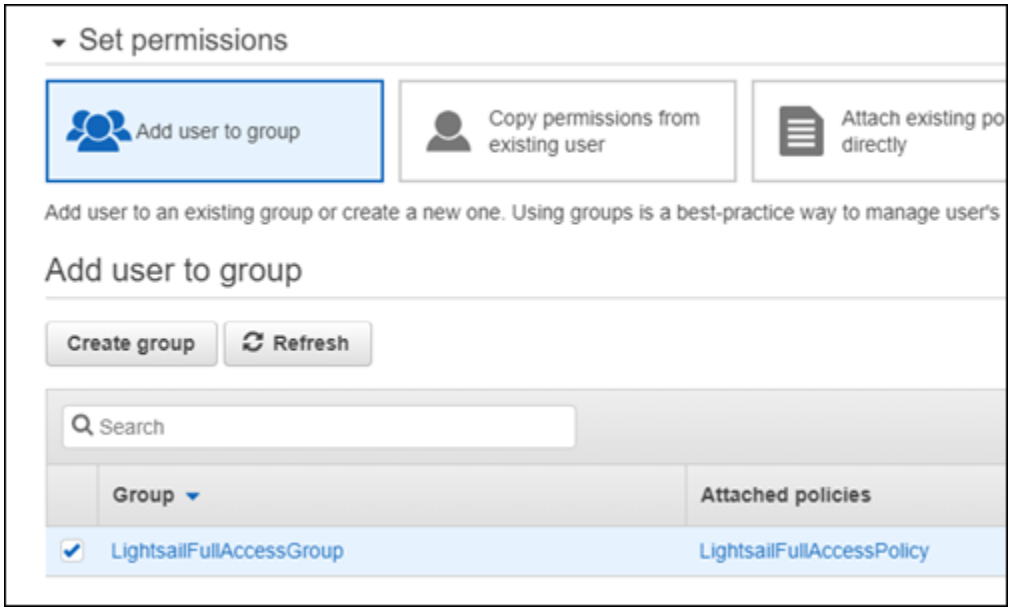
   b. Wählen Sie AWS Management Console access (Zugriff auf die Verwaltungskonsole), um den Zugriff auf ein Passwort zu aktivieren, das es dem Benutzer ermöglicht, Sie sich bei der AWS-Verwaltungskonsole und somit bei der Lightsail-Konsole anzumelden. Die folgenden Passwortoptionen werden angezeigt, wenn diese Option ausgewählt wird:

      i. Wählen Sie Automatisch generiertes Passwort, damit IAM das Passwort generiert, oder wählen Sie „Benutzerdefiniertes Passwort“ aus, um Ihr eigenes Passwort eingeben.

      ii. Wählen Sie Require password reset (Passwort-Rücksetzung erforderlich) aus, damit der Benutzer bei der nächsten Anmeldung ein neues Passwort erstellen (sein Passwort zurücksetzen) muss.

> **Note**
>
> Wenn Sie nur die Option Programmatic Access (Programmzugriff) auswählen, kann sich der Benutzer nicht bei der AWS-Konsole und der Lightsail-Konsole anmelden.

5. Wählen Sie Next: Permissions (Weiter: Berechtigungen) aus.
6. Wählen Sie auf der Seite im Abschnitt Set permissions (Berechtigungen einstellen) die Option Add user to group (Benutzer zur Gruppe hinzufügen) aus, und wählen Sie dann die Lightsail-Zugriffsgruppe, die Sie zuvor in dieser Anleitung erstellt haben, z. B. `LightsailFullAccessGroup`.



7. Wählen Sie Next: Tags (Weiter: Tags) aus.
8. (Optional) Fügen Sie dem Benutzer Metadaten hinzu, indem Sie Markierungen als Schlüssel-Wert-Paare anfügen. Weitere Informationen zur Verwendung von Tags in IAM finden Sie unter Tagging von IAM-Entitäten.
9. Wählen Sie Weiter: Prüfen aus.
10. Überprüfen Sie die Benutzereinstellungen. Wenn Sie Änderungen vornehmen müssen, wählen Sie Previous (Zurück), um die Gruppen oder Richtlinien des Benutzers zu ändern.
11. Wenn die Benutzereinstellungen korrekt sind, wählen Sie Create user (Benutzer erstellen) aus.

    Der Benutzer wird erstellt, und der Benutzer kann auf Lightsail zugreifen. Um den Zugriff des Benutzers auf Lightsail zu widerrufen, entfernen Sie den Benutzer aus der Lightsail-

Zugriffsgruppe. Weitere Informationen finden Sie unter Hinzufügen und Entfernen von Benutzern in einer IAM-Gruppe in der IAM-Dokumentation.

12. Um die Anmeldeinformationen des Benutzers abzurufen, wählen Sie die folgenden Optionen:

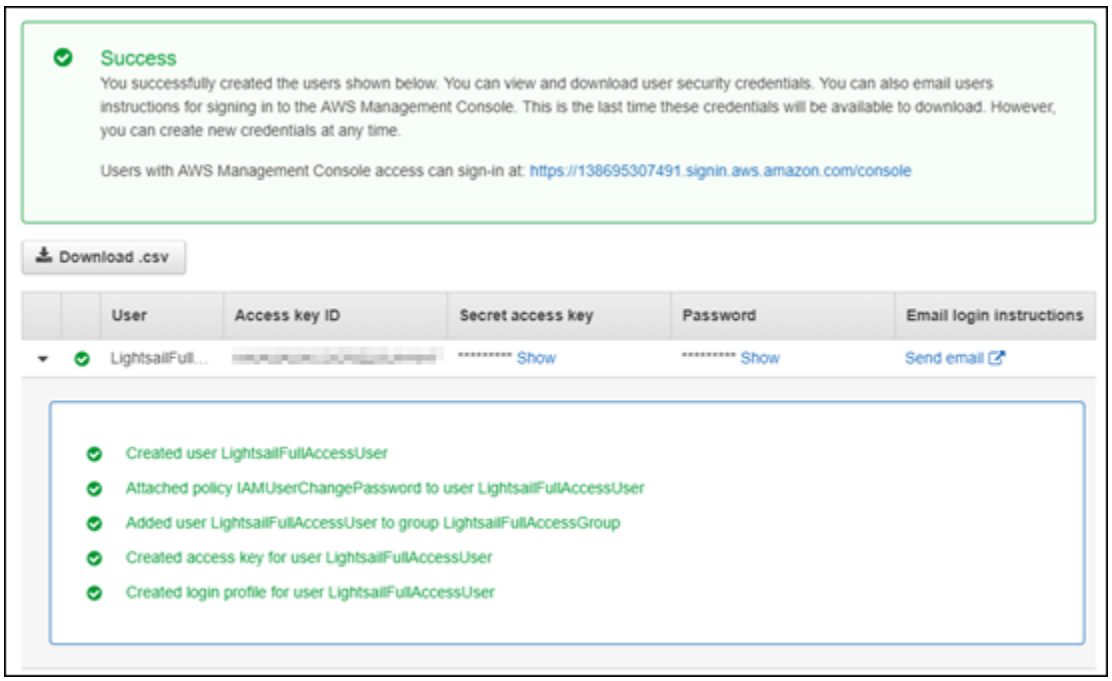
    a. Wählen Sie Download .csv (csv herunterladen), um eine Datei mit dem Benutzernamen, Passwort, Zugriffsschlüssel-ID, geheimen Zugriffsschlüssel und den Anmelde-Link für die AWS-Konsole Ihres Kontos herunterzuladen.

    b. Wählen Sie Show (Anzeigen) unter Secret access key (Geheimer Zugriffsschlüssel), um die Zugriffsschlüssel anzeigen, die verwendet werden können, um programmgesteuert auf Lightsail (mithilfe der AWS API, CLI, SDK und anderen Entwicklungstools) zuzugreifen.

    > **Important**
    >
    > Dies ist die einzige Gelegenheit, die geheimen Zugriffsschlüssel anzuzeigen oder herunterzuladen, und Sie müssen Ihren Benutzern diese Informationen bereitstellen, damit sie die AWS-API verwenden können. Speichern Sie die neue Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel des Benutzers an einem sicheren Speicherort. Sie haben nach diesem Schritt keinen Zugriff mehr auf die geheimen Zugriffsschlüssel.

    c. Wählen Sie Anzeigen unter Passwort, um das Passwort des Benutzers anzuzeigen, wenn es von IAM automatisch generiert wurde. Sie sollten das Passwort für die Benutzer bereitstellen, damit sie sich das erste Mal anmelden können.

    d. Wählen Sie Send email (E-Mail senden), um die Benutzer darüber zu informieren, dass Sie jetzt Zugriff auf Lightsail haben.



Update-Management in Amazon Lightsail

Amazon Web Services (AWS), Amazon Lightsail und Drittanbieter von Anwendungen aktualisieren und patchen regelmäßig die Instance-Images (auch bekannt als Vorlagen), die auf Lightsail verfügbar sind. AWS und Lightsail aktualisieren oder patchen das Betriebssystem oder die Anwendungen auf Instances nicht, nachdem Sie sie erstellt haben. Lightsail aktualisiert oder patcht auch nicht das Betriebssystem und die Software, die Sie auf Ihren Lightsail-Container-Services konfigurieren. Wir empfehlen Ihnen deshalb, das Betriebssystem und die Anwendungen auf Ihren Amazon Lightsail-Instances und Containerservices regelmäßig zu patchen, zu aktualisieren und zu sichern. Weitere Informationen finden Sie unter AWS-Modell der geteilten Verantwortung.

Softwaresupport für Instance-Vorlagen

Die folgende Liste mit Amazon Lightsail-Plattformen und Vorlagen verlinkt auf die Support-Seiten der einzelnen Anbieter. Dort können Sie Informationen wie Anleitungen anzeigen und Ihr Betriebssystem und Ihre Anwendung auf dem neuesten Stand halten. Sie können jeden automatischen Update-Service oder empfohlenen Prozess zum Installieren von Updates verwenden, die vom Anwendungsanbieter bereitgestellt werden.

Windows

- Windows Server 2022, Windows Server 2019, Windows Server 2016 und Windows Server 2012 R2

- Microsoft SQL Server

Linux und Unix – Nur Betriebssystem

- Amazon Linux 2023
- Amazon Linux 2
- Ubuntu
- Debian
- FreeBSD
- openSUSE
- CentOS

Linux und Unix – Betriebssystem plus Anwendung

- Plesk Hosting-Stack auf Ubuntu
- cPanel & WHM für Linux
- WordPress
- WordPress Multisite
- LAMP (PHP 8)
- Node.js
- Joomla!
- Magento
- MEAN
- Drupal
- GitLab CE
- Redmine
- Nginx
- Ghost
- Django
- PrestaShop

Compliance-Validierung für Amazon Lightsail

AWS stellt die folgenden Ressourcen bereit, um Sie bei der Compliance zu unterstützen:

- Kurzanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden finden Sie wichtige Überlegungen zur Architektur sowie die einzelnen Schritte zur Bereitstellung von sicherheits- und Compliance-orientierten Basisumgebungen in AWS.
- AWS-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort interessant sein.
- Auswertung von Ressourcen mit Regeln im AWS ConfigEntwicklerhandbuch – Der AWS Config-Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub – Dieser AWS-Service liefert einen umfassenden Überblick über den Sicherheitsstatus in AWS. So können Sie die Compliance mit den Sicherheitsstandards in der Branche und den bewährten Methoden abgleichen.

Überwachen Sie Ihre Amazon Lightsail-Ressourcen

Überwachen Sie die Leistung Ihrer Instances, Datenbanken, Verteilungen, Load Balancers, Containerdienste und Buckets in Amazon Lightsail, indem Sie ihre Metrikdaten überprüfen und sammeln. Legen Sie im Laufe der Zeit einen Bereich fest, damit Sie Alarme konfigurieren können, um Anomalien und Probleme mit der Leistung Ihrer Ressourcen leichter zu erkennen.

Amazon Lightsail meldet Metrikdaten für Instances, Datenbanken, Bereitstellung von Content Delivery Network (CDN), Load Balancers, Containerdienste und Buckets. Sie können diese Daten in der Lightsail-Konsole anzeigen und überwachen. Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Performance Ihrer -Ressourcen aufrechtzuerhalten. Überwachen und sammeln Sie regelmäßig Metrikdaten von Ihren Ressourcen, damit Sie bei Auftreten eines Mehrpunkt-Fehlers diesen leichter debuggen können.

Inhalt

Effektive Überwachung Ihrer Ressourcen

Legen Sie einen Bereich für die normale Ressourcenleistung in Ihrer Umgebung fest. Messen Sie die Leistung zu verschiedenen Zeiten und unter verschiedenen Belastungsbedingungen. Während der Überwachung Ihrer Ressourcen sollten Sie einen Verlauf der Leistung Ihrer Ressource im Laufe der Zeit notieren und diesen aufzeichnen. Vergleichen Sie die aktuelle Leistung Ihrer Ressourcen mit den von Ihnen gesammelten historischen Daten. Auf diese Weise können Sie normale Leistungsmuster und Leistungsanomalien identifizieren und Methoden entwickeln, um diese zu beheben.

Beispielsweise können Sie CPU-Auslastung, Netzwerkauslastung und Statusüberprüfungen für Ihre Instances überwachen. Wenn die Leistung außerhalb der festgelegten Bereiche liegt, müssen Sie die Instance neu konfigurieren oder optimieren, um die CPU-Nutzung zu verringern oder den Netzwerkverkehr zu reduzieren. Wenn Ihre Instance die CPU-Auslastungsschwellenwerte weiterhin überschreitet, können Sie zu einem höheren Tarif für Ihre Instance wechseln (z. B. Tarif für 5 USD/Monat anstelle des Tarifs für 3,50 USD/Monat). Sie können zu einem höheren Tarif wechseln, indem Sie einen neuen Snapshot Ihrer Instance erstellen und dann mithilfe des höheren Tarifs eine neue Instance aus dem Snapshot erstellen.

Nachdem Sie einen Bereich eingerichtet haben, können Sie Alarme in der Lightsail-Konsole konfigurieren, damit Sie benachrichtigt werden, wenn Ihre Ressourcen die angegebenen Schwellenwerte überschreiten. Weitere Informationen finden Sie unter Benachrichtigungen und Alarme.

Metrikkonzepte und -terminologie

Die folgenden Begriffe und Konzepte helfen Ihnen, die Verwendung von Metriken in Lightsail besser zu verstehen.

Metriken

Eine Metrik stellt einen chronologisch sortierten Satz von Datenpunkten dar. Sie können sich eine Metrik als eine zu überwachende Variable und die Datenpunkte als die Werte dieser Variablen im Laufe der Zeit vorstellen. Metriken werden durch einen Namen eindeutig definiert. Beispielsweise umfassen einige Instance-Metriken, die von Lightsail bereitgestellt werden, die CPU-Auslastung (`CPUUtilization`), den eingehenden Netzwerkverkehr (`NetworkIn`) und den ausgehenden Netzwerkverkehr (`NetworkOut`). Weitere Informationen zu allen Ressourcenmetriken, die in Lightsail verfügbar sind, finden Sie unter In Lightsail verfügbare Metriken.

Speicherung von Metriken

Datenpunkte mit einem Zeitraum von 60 Sekunden (Auflösung 1 Minute) stehen 15 Tage lang zur Verfügung. Datenpunkte mit einem Zeitraum von 300 Sekunden (Auflösung 5 Minuten) stehen 63 Tage lang zur Verfügung. Datenpunkte mit einem Zeitraum von 3 600 Sekunden (Auflösung 1 Stunde) stehen 455 Tage (15 Monate) lang zur Verfügung.

Datenpunkte, die ursprünglich für kürzere Zeit verfügbar waren, werden für eine langfristige Speicherung aggregiert. Beispielsweise bleiben Datenpunkte mit einer Granularität von 1 Minute 15 Tage lang mit einer Auflösung von 1 Minute verfügbar. Nach 15 Tagen sind die Daten noch immer verfügbar, aber sie sind aggregiert und können nur mit einer Auflösung von 5 Minuten abgerufen werden. Nach 63 Tagen werden die Daten weiter aggregiert und sind nur mit einer Auflösung von 1 Stunde verfügbar. Sollen Ihre Metriken über diese Standardzeiträume hinaus weiterhin verfügbar sein, können Sie diese Datenpunkte mit der Lightsail-API, AWS Command Line Interface (AWS CLI) und SDKs abrufen und offline oder an einem anderen Speicherort ablegen.

Weitere Informationen finden Sie unter GetInstanceMetricData, GetBucketMetricData, GetLoadBalancerMetricData, GetDistributionMetricData und GetRelationalDatabaseMetricData in der Lightsail-API-Referenz.

Statistiken

In Metrikstatistiken werden Daten über einen bestimmten Zeitraum aggregiert. Beispielstatistiken sind `Average`, `Sum` und `Maximum`. Beispiel: Instance-CPU-Auslastungsmetrikdaten können mithilfe der `Average`-Statistik gemittelt werden, Datenbankverbindungen können mithilfe der `Sum`-Statistik hinzugefügt werden, die maximale Antwortzeit für den Load Balancer kann mithilfe der `Maximum`-Statistik abgerufen werden usw.

Eine Liste der verfügbaren Metrikstatistiken finden Sie unter Statistiken für GetInstanceMetricData, Statistiken für GetBucketMetricData, Statistiken für GetLoadBalancerMetricData, Statistiken für GetDistributionMetricData und Statistiken für GetRelationalDatabaseMetricData in der Lightsail-API-Referenz.

Einheiten

Jede Statistik verfügt über eine Maßeinheit. Zu den Einheiten gehören beispielsweise `Bytes`, `Seconds`, `Count` und `Percent`. Eine vollständige Liste der Einheiten finden Sie unter Einheiten für GetInstanceMetricData, Einheiten für GetLoadBalancerMetricData, Einheiten für GetDistributionMetricData und Einheiten für GetRelationalDatabaseMetricData in der Lightsail-API-Referenz.

Zeiträume

Ein Zeitraum ist die mit einem bestimmten Datenpunkt verbundene Zeitdauer – die Granularität der zurückgegebenen Datenpunkte. Jeder Datenpunkt stellt eine Aggregation der Metrikdaten dar, die über einen bestimmten Zeitraum erfasst wurden. Zeiträume werden in Sekunden definiert, und die gültigen Werte für Zeiträume sind Vielfache von 60 Sekunden (1 Minute) und 300 Sekunden (5 Minuten).

Wenn Sie Datenpunkte mithilfe der Lightsail-API abrufen, können Sie einen Zeitraum, eine Startzeit und eine Endzeit angeben. Diese Parameter bestimmen die allgemeine mit den Statistiken verbundene Dauer. Lightsail meldet Metrikdaten entweder in Schritten von 1 Minute oder 5 Minuten. Daher müssen Sie Perioden in Vielfachen von 60 Sekunden und 300 Sekunden angeben. Die Werte, die Sie als Start- und Endzeit festlegen, bestimmen, wie viele Zeiträume von Lightsail zurückgegeben werden. Wenn Sie lieber Statistiken haben möchten, die in Blöcke von 10 Minuten zusammengefasst sind, geben Sie einen Zeitraum von 600 an. Für Statistiken, die über die gesamte Stunde aggregiert sind, geben Sie einen Zeitraum von 3 600 usw. an.

Zeiträume sind auch für Lightsail-Alarme wichtig. Lightsail wertet alle 5 Minuten Datenpunkte für Alarme aus, wobei jeder Datenpunkt einen 5-minütigen Zeitraum aggregierter Daten darstellt. Wenn Sie einen Alarm einrichten, um eine bestimmte Metrik zu überwachen, fordern Sie Lightsail auf, diese Metrik mit dem Schwellenwert, den Sie angeben, zu vergleichen. Sie haben umfassende Kontrolle darüber, wie Lightsail diesen Vergleich vornimmt. Sie können den Zeitraum angeben, über den der Vergleich erfolgen soll, und zudem angeben, wie viele Auswertungszeiträume verwendet werden, um zu einer Schlussfolgerung zu gelangen. Weitere Informationen finden Sie unter -Alarme.

Alarme

Ein Alarm überwacht eine einzelne Metrik über einen bestimmten Zeitraum und benachrichtigt Sie, wenn die Metrik einen von Ihnen festgelegten Schwellenwert überschreitet. Die Benachrichtigung kann ein Banner sein, das in der Lightsail-Konsole angezeigt wird, eine E-Mail, die an eine von Ihnen angegebene E-Mail-Adresse gesendet wird, und eine SMS-Textnachricht, die an eine von Ihnen angegebene Mobiltelefonnummer gesendet wird. Weitere Informationen finden Sie unter -Alarme.

Metriken verfügbar in Lightsail

Instance-Metriken

Die folgenden Instance-Metriken sind verfügbar. Weitere Informationen finden Sie unter Anzeigen von Instance-Metriken in Amazon Lightsail.

- CPU-Auslastung (**`CPUUtilization`**) – Der Prozentsatz der zugeordneten Recheneinheiten, die derzeit auf der Instance verwendet werden. Diese Metrik identifiziert die Verarbeitungsleistung für die Ausführung der Anwendungen auf der Instance. Die Tools Ihres Betriebssystems können geringere Prozentsätze als Lightsail anzeigen, wenn der Instance kein vollständiger Prozessorkern zugeordnet ist.

  Wenn Sie die Metrik-Diagramme für die CPU-Auslastung für Ihre Instances in der Lightsail-Konsole anzeigen, werden nachhaltige und burstfähige Zonen angezeigt. Weitere Informationen zur Bedeutung dieser Zonen finden Sie unter CPU-Auslastung in nachhaltigen und burstfähigen Zonen.
- Burst-Kapazitätsminuten (**`BurstCapacityTime`**) und Prozentsatz (**`BurstCapacityPercentage`**) – Burst-Kapazitätsminuten stellen die Zeit dar, die Ihrer Instance für das Bursten bei 100 % CPU-Auslastung zur Verfügung steht. Der Prozentsatz der Burst-Kapazität ist der Prozentsatz der CPU-Leistung, die Ihrer Instance zur Verfügung steht. Ihre Instance verbraucht kontinuierlich Burst-Kapazität und sammelt diese an. Die Burst-Kapazitätsminuten werden nur dann mit voller Geschwindigkeit verbraucht, wenn Ihre Instance mit

100 % CPU-Auslastung arbeitet. Weitere Informationen zur Instance-Burst-Kapazität finden Sie unter Anzeigen von Instance-Burst-Kapazität in Amazon Lightsail.

- Eingehender Netzwerkdatenverkehr (**`NetworkIn`**) – Die Anzahl der Bytes, die von der Instance an allen Netzwerkschnittstellen empfangen wurde. Diese Metrik gibt das eingehende Netzwerkdatenvolumen an der Instance an. Der ermittelte Wert ist die Anzahl der während des Zeitraums empfangenen Byte. Da diese Metrik in 5-Minuten-Intervallen gemeldet wird, teilen Sie die gemeldete Zahl durch 300, um Byte/Sekunde zu erhalten.
- Ausgehender Netzwerkdatenverkehr (**`NetworkOut`**) – Die Anzahl der Bytes, die von der Instance an allen Netzwerkschnittstellen versandt wurde. Diese Metrik gibt das ausgehende Netzwerkdatenvolumen an einer Instance an. Der ermittelte Wert ist die Anzahl der während des Zeitraums gesendeten Bytes. Da diese Metrik in 5-Minuten-Intervallen gemeldet wird, teilen Sie die gemeldete Zahl durch 300, um Byte/Sekunde zu erhalten.
- Fehler bei der Zustandsprüfung (**`StatusCheckFailed`**) – Berichtet, ob die Instance sowohl die Instance-Statusprüfung als auch die System-Statusprüfung bestanden hat oder nicht. Diese Metrik nimmt den Wert 0 (bestanden) oder 1 (fehlgeschlagen) an. Diese Metrik ist mit einer einminütigen Frequenz verfügbar.
- Fehler bei der Instance-Statusprüfung (**`StatusCheckFailed_Instance`**) – Berichtet, ob die Instance die Instance-Statusprüfung bestanden hat oder nicht. Diese Metrik nimmt den Wert 0 (bestanden) oder 1 (fehlgeschlagen) an. Diese Metrik ist mit einer einminütigen Frequenz verfügbar.
- Fehler bei der System-Statusprüfung (**`StatusCheckFailed_System`**) – Berichtet, ob die Instance die System-Statusprüfung bestanden hat oder nicht. Diese Metrik nimmt den Wert 0 (bestanden) oder 1 (fehlgeschlagen) an. Diese Metrik ist mit einer einminütigen Frequenz verfügbar.
- Keine Token-Metadatenanforderungen (**`MetadataNoToken`**) – Gibt an, wie oft erfolgreich ohne Token auf den Instance-Metadatenservice zugegriffen wurde. Diese Metrik bestimmt, ob Prozesse vorhanden sind, die mit Instance-Metadatenservice Version 1, das keinen Token verwendet, auf Instance-Metadaten zugreifen. Wenn alle Anfragen Token-gestützte Sitzungen verwenden, d. h. Instance-Metadatenservice Version 2, ist der Wert 0. Weitere Informationen finden Sie unter Instance-Metadaten und Benutzerdaten im Amazon Lightsail.

Datenbankmetriken

Die folgenden Datenbankmetriken sind verfügbar. Weitere Informationen finden Sie unter Anzeigen von Datenbankmetriken in Amazon Lightsail.

- CPU-Auslastung (**`CPUUtilization`**) – Prozentsatz der CPU-Auslastung, die gegenwärtig in der Datenbank verwendet wird.
- Datenbankverbindungen (**`DatabaseConnections`**) – Anzahl der genutzten Datenbankverbindungen.
- Tiefe der Datenträgerwarteschlange (**`DiskQueueDepth`**) – Anzahl der offenstehenden E/A (Lese-/Schreibanforderungen), die auf den Datenträger zugreifen möchten.
- Freier Speicherplatz (**`FreeStorageSpace`**) – Die Menge an verfügbarem Speicherplatz.
- Netzwerkempfangsdurchsatz (**`NetworkReceiveThroughput`**) – Der eingehende (Receive) Netzwerkverkehr auf der Datenbank, einschließlich Kundendatenbankverkehr und AWS-Datenverkehr, der für Überwachung und Replikation verwendet wird.
- Netzwerkausgangsdurchsatz (**`NetworkTransmitThroughput`**) – Der ausgehende (Transmit) Netzwerkverkehr auf der Datenbank, einschließlich Kundendatenbankverkehr und AWS-Datenverkehr, der für Überwachung und Replikation verwendet wird.

Verteilungsmetriken

Folgende Verteilungsmetriken sind verfügbar. Weitere Informationen finden Sie unter Anzeigen von Verteilungsmetriken in Amazon Lightsail.

- Anforderungen (**`Requests`**) – Die Gesamtzahl der von Ihrer Verteilung empfangenen Viewer-Anforderungen für alle HTTP-Methoden sowie für HTTP- und HTTPS-Anforderungen.
- Hochgeladene Bytes (**`BytesUploaded`**) – Die Anzahl der Bytes, die von Ihrer Verteilung mithilfe von POST- und PUT-Anforderungen an Ihren Ursprung hochgeladen wurden.
- Heruntergeladene Bytes (**`BytesDownloaded`**) – Die Anzahl der von Viewern für GET-, HEAD- und OPTIONS-Anforderungen heruntergeladenen Bytes.
- Fehlerrate gesamt (**`TotalErrorRate`**) – Der Prozentsatz aller Viewer-Anforderungen, für die der HTTP-Statuscode der Antwort 4xx oder 5xx lautet.
- HTTP-4xx-Fehlerrate (**`4xxErrorRate`**) – Der Prozentsatz aller Viewer-Anforderungen, für die der HTTP-Statuscode der Antwort 4xx lautet. In diesen Fällen hat der Client oder Client-Viewer möglicherweise einen Fehler gemacht. Beispiel: 404 (nicht gefunden) bedeutet, dass der Client ein Objekt angefordert hat, das nicht gefunden wurde.
- HTTP-5xx-Fehlerrate (**`5xxErrorRate`**) – Der Prozentsatz aller Viewer-Anforderungen, für die der HTTP-Statuscode der Antwort 5xx lautet. In diesen Fällen hat der Ursprungsserver die Anforderung nicht erfüllt. Beispiel: 503 (Service nicht verfügbar) bedeutet, dass der Ursprungsserver zurzeit nicht verfügbar ist.

Load Balancer-Metriken

Die folgenden Load Balancer-Metriken sind verfügbar. Weitere Informationen finden Sie unter Anzeigen von Load Balancer-Metriken in Amazon Lightsail.

- Fehlerfreie Hostanzahl (**`HealthyHostCount`**) – Die Anzahl der Ziel-Instances, die als fehlerfrei betrachtet werden.
- Anzahl fehlerhafter Hosts (**`UnhealthyHostCount`**) – Die Anzahl der Ziel-Instances, die als fehlerhaft betrachtet werden.
- Load Balancer HTTP-4XX (**`HTTPCode_LB_4XX_Count`**) – Anzahl von HTTP-4XX-Client-Fehlercodes, die von Load Balancern verursacht werden. Client-Fehler werden bei Anforderungen mit falschem Format oder unvollständigen Anforderungen generiert. Diese Anforderungen wurden von der Ziel-Instance nicht empfangen. Diese Anzahl umfasst keine Antwortcodes, die von den Ziel-Instances generiert wurden.
- Load Balancer-HTTP-5XX (**`HTTPCode_LB_5XX_Count`**) – Anzahl von HTTP-5XX-Server-Fehlercodes, die von Load Balancern verursacht werden. Hierin sind keine von der Ziel-Instance generierten Antwortcodes enthalten. Die Metrik wird gemeldet, wenn für den Load Balancer keine fehlerfreien Instances angefügt sind oder wenn die Anforderungsrate die Kapazität der Instances (Überlauf) oder des Load Balancers überschreitet.
- HTTP-2XX-Instance (**`HTTPCode_Instance_2XX_Count`**) – Die Anzahl der HTTP-2XX-Antwortcodes, die von den Ziel-Instances generiert werden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.
- HTTP-3XX-Instance (**`HTTPCode_Instance_3XX_Count`**) – Die Anzahl der HTTP-3XX-Antwortcodes, die von den Ziel-Instances generiert werden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.
- HTTP-4XX-Instance (**`HTTPCode_Instance_4XX_Count`**) – Die Anzahl der HTTP-4XX-Antwortcodes, die von den Ziel-Instances generiert werden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.
- HTTP-5XX-Instance (**`HTTPCode_Instance_5XX_Count`**) – Die Anzahl der HTTP-5XX-Antwortcodes, die von den Ziel-Instances generiert werden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.
- Instance-Antwortzeit (**`InstanceResponseTime`**) – Die verstrichene Zeit in Sekunden bis zum Empfang einer Antwort von der Ziel-Instance, nachdem die Anforderung den Load Balancer verlassen hat.

- Fehlerzahl-Client-TLS-Vereinbarung (**`ClientTLSNegotiationErrorCount`**) – Die Anzahl der vom Client initiierten TLS-Verbindungen, die keine Sitzung mit de Load Balancer eingerichtet haben, da der Load Balancer einen TLS-Fehler generiert hat. Als mögliche Ursachen kommen unter anderem fehlende Übereinstimmung bei Verschlüsselungsverfahren oder Protokollen infrage.
- Anzahl der Anforderungen (**`RequestCount`**) – Die Anzahl von Anforderungen, die über IPv4 verarbeitet wurden. In dieser Zahl sind nur die Anforderungen mit einer Antwort enthalten, die von einer Ziel-Instance des Load Balancers generiert wurden.
- Anzahl der abgelehnten Verbindungen (**`RejectedConnectionCount`**) Die Anzahl der abgelehnten Verbindungen, weil der Load Balancer die maximale Anzahl an Verbindungen erreicht hat.

Container-Service-Metriken

Die folgenden Containermetriken sind verfügbar. Weitere Informationen finden Sie unter Anzeigen von Container-Services-Metriken.

- CPU-Nutzung (**`CPUUtilization`**) – Der durchschnittliche Prozentsatz der Recheneinheiten, die gegenwärtig auf allen Knoten Ihres Container-Services verwendet werden. Diese Metrik gibt die erforderliche Rechenleistung an, um Container-Services auszuführen.
- Speicherauslastung (**`MemoryUtilization`**) – Der durchschnittliche Prozentsatz des Arbeitsspeichers, der derzeit auf allen Knoten des Container-Services verwendet wird. Diese Metrik identifiziert den Speicher, der zum Ausführen von Containern in Ihrem Containerdienst erforderlich ist.

Bucket-Metriken

Die folgenden Metriken sind verfügbar. Weitere Informationen finden Sie unter Anzeigen von Instance-Metriken in Amazon Lightsail.

- Bucket-Größe (**`BucketSizeBytes`**) – Die Menge der in einem Bucket gespeicherten Daten. Zur Berechnung dieses Werts wird die Größe aller (aktuellen und nicht aktuellen) Objekte im Bucket summiert – einschließlich der Größe aller Teile für sämtliche unvollständige mehrteilige Uploads in den Bucket.
- Anzahl Objekte (**`NumberOfObjects`**) – Die Gesamtzahl der Objekte, die in einem Bucket gespeichert sind. Zur Berechnung dieses Werts werden alle aktuellen und nicht aktuellen Objekte

im Bucket sowie die Gesamtanzahl der Teile sämtlicher unvollständiger mehrteiliger Uploads in den Bucket gezählt.

> **Note**
>
> Bucket-Metrikdaten werden nicht gemeldet, wenn Ihr Bucket leer ist.

Lightsail-Metriken zum Ressourcenzustand

Sie können die folgenden Amazon Lightsail-Ressourcenmetriken über verschiedene Zeiträume anzeigen. Weitere Informationen zu Ressourcenmetriken in Lightsail finden Sie unter Ressourcenmetriken.

Instance-Metriken

Die folgenden Instance-Metriken sind verfügbar. Weitere Informationen finden Sie unter Anzeigen von Instance-Metriken in Amazon Lightsail.

- CPU-Auslastung (**`CPUUtilization`**) – Der Prozentsatz der zugeordneten Recheneinheiten, die derzeit auf der Instance verwendet werden. Diese Metrik identifiziert die Verarbeitungsleistung für die Ausführung der Anwendungen auf der Instance. Die Tools Ihres Betriebssystems können geringere Prozentsätze als Lightsail anzeigen, wenn der Instance kein vollständiger Prozessorkern zugeordnet ist.

  Wenn Sie die Metrik-Diagramme für die CPU-Auslastung für Ihre Instances in der Lightsail-Konsole anzeigen, werden nachhaltige und burstfähige Zonen angezeigt. Weitere Informationen zur Bedeutung dieser Zonen finden Sie unter CPU-Auslastung in nachhaltigen und burstfähigen Zonen.
- Burst-Kapazitätsminuten (**`BurstCapacityTime`**) und Prozentsatz (**`BurstCapacityPercentage`**) – Burst-Kapazitätsminuten stellen die Zeit dar, die Ihrer Instance für das Bursten bei 100 % CPU-Auslastung zur Verfügung steht. Der Prozentsatz der Burst-Kapazität ist der Prozentsatz der CPU-Leistung, die Ihrer Instance zur Verfügung steht. Ihre Instance verbraucht kontinuierlich Burst-Kapazität und sammelt diese an. Die Burst-Kapazitätsminuten werden nur dann mit voller Geschwindigkeit verbraucht, wenn Ihre Instance mit 100 % CPU-Auslastung arbeitet. Weitere Informationen zur Instance-Burst-Kapazität finden Sie unter Anzeigen von Instance-Burst-Kapazität.

- Eingehender Netzwerkdatenverkehr (**`NetworkIn`**) – Die Anzahl der Bytes, die von der Instance an allen Netzwerkschnittstellen empfangen wurde. Diese Metrik gibt das eingehende Netzwerkdatenvolumen an der Instance an. Der ermittelte Wert ist die Anzahl der während des Zeitraums empfangenen Byte. Da diese Metrik in 5-Minuten-Intervallen gemeldet wird, teilen Sie die gemeldete Zahl durch 300, um Byte/Sekunde zu erhalten.
- Ausgehender Netzwerkdatenverkehr (**`NetworkOut`**) – Die Anzahl der Bytes, die von der Instance an allen Netzwerkschnittstellen versandt wurde. Diese Metrik gibt das ausgehende Netzwerkdatenvolumen an einer Instance an. Der ermittelte Wert ist die Anzahl der während des Zeitraums gesendeten Bytes. Da diese Metrik in 5-Minuten-Intervallen gemeldet wird, teilen Sie die gemeldete Zahl durch 300, um Byte/Sekunde zu erhalten.
- Fehler bei der Zustandsprüfung (**`StatusCheckFailed`**) – Berichtet, ob die Instance sowohl die Instance-Statusprüfung als auch die System-Statusprüfung bestanden hat oder nicht. Diese Metrik nimmt den Wert 0 (bestanden) oder 1 (fehlgeschlagen) an. Diese Metrik ist mit einer einminütigen Frequenz verfügbar.
- Fehler bei der Instance-Statusprüfung (**`StatusCheckFailed_Instance`**) – Berichtet, ob die Instance die Instance-Statusprüfung bestanden hat oder nicht. Diese Metrik nimmt den Wert 0 (bestanden) oder 1 (fehlgeschlagen) an. Diese Metrik ist mit einer einminütigen Frequenz verfügbar.
- Fehler bei der System-Statusprüfung (**`StatusCheckFailed_System`**) – Berichtet, ob die Instance die System-Statusprüfung bestanden hat oder nicht. Diese Metrik nimmt den Wert 0 (bestanden) oder 1 (fehlgeschlagen) an. Diese Metrik ist mit einer einminütigen Frequenz verfügbar.
- Fehler bei der System-Statusprüfung (**`StatusCheckFailed_System`**) – Berichtet, ob die Instance die System-Statusprüfung bestanden hat oder nicht. Diese Metrik nimmt den Wert 0 (bestanden) oder 1 (fehlgeschlagen) an. Diese Metrik ist mit einer einminütigen Frequenz verfügbar.
- Keine Token-Metadatenanforderungen (**`MetadataNoToken`**) – Gibt an, wie oft erfolgreich ohne Token auf den Instance-Metadatenservice zugegriffen wurde. Diese Metrik bestimmt, ob Prozesse vorhanden sind, die mit Instance-Metadatenservice Version 1, das keinen Token verwendet, auf Instance-Metadaten zugreifen. Wenn alle Anfragen Token-gestützte Sitzungen verwenden, d. h. Instance-Metadatenservice Version 2, ist der Wert 0. Weitere Informationen finden Sie unter Instance-Metadaten und Benutzerdaten.

Datenbankmetriken

Die folgenden Datenbankmetriken sind verfügbar. Weitere Informationen finden Sie unter Anzeigen von Datenbankmetriken.

- CPU-Auslastung (**`CPUUtilization`**) – Prozentsatz der CPU-Auslastung, die gegenwärtig in der Datenbank verwendet wird.
- Datenbankverbindungen (**`DatabaseConnections`**) – Anzahl der genutzten Datenbankverbindungen.
- Tiefe der Datenträgerwarteschlange (**`DiskQueueDepth`**) – Anzahl der offenstehenden E/A (Lese-/Schreibanforderungen), die auf den Datenträger zugreifen möchten.
- Freier Speicherplatz (**`FreeStorageSpace`**) – Die Menge an verfügbarem Speicherplatz.
- Netzwerkempfangsdurchsatz (**`NetworkReceiveThroughput`**) – Der eingehende (Receive) Netzwerkverkehr auf der Datenbank, einschließlich Kundendatenbankverkehr und AWS-Datenverkehr, der für Überwachung und Replikation verwendet wird.
- Netzwerkausgangsdurchsatz (**`NetworkTransmitThroughput`**) – Der ausgehende (Transmit) Netzwerkverkehr auf der Datenbank, einschließlich Kundendatenbankverkehr und AWS-Datenverkehr, der für Überwachung und Replikation verwendet wird.

Verteilungsmetriken

Folgende Verteilungsmetriken sind verfügbar. Weitere Informationen finden Sie unter Anzeigen von Verteilungsmetriken in Amazon Lightsail.

- Anforderungen – Die Gesamtzahl der von Ihrer Verteilung empfangenen Viewer-Anforderungen für alle HTTP-Methoden sowie für HTTP- und HTTPS-Anforderungen.
- Hochgeladene Bytes – Die Anzahl der Bytes, die von Ihrer Verteilung mithilfe von POST- und PUT-Anforderungen an Ihren Ursprung hochgeladen wurden.
- Heruntergeladene Bytes – Die Anzahl der von Viewern für GET-, HEAD- und OPTIONS-Anforderungen heruntergeladenen Bytes.
- Fehlerrate gesamt – Der Prozentsatz aller Viewer-Anforderungen, für die der HTTP-Statuscode der Antwort 4xx oder 5xx lautet.
- HTTP-4xx-Fehlerrate – Der Prozentsatz aller Viewer-Anforderungen, für die der HTTP-Statuscode der Antwort 4xx lautet. In diesen Fällen hat der Client oder Client-Viewer möglicherweise einen

Fehler gemacht. Beispiel: 404 (nicht gefunden) bedeutet, dass der Client ein Objekt angefordert hat, das nicht gefunden wurde.

- HTTP-5xx-Fehlerrate – Der Prozentsatz aller Viewer-Anforderungen, für die der HTTP-Statuscode der Antwort 5xx lautet. In diesen Fällen hat der Ursprungsserver die Anforderung nicht erfüllt. Beispiel: 503 (Service nicht verfügbar) bedeutet, dass der Ursprungsserver zurzeit nicht verfügbar ist.

Load Balancer-Metriken

Die folgenden Load Balancer-Metriken sind verfügbar. Weitere Informationen finden Sie unter Anzeigen von Load Balancer-Metriken.

- Fehlerfreie Hostanzahl (**`HealthyHostCount`**) – Die Anzahl der Ziel-Instances, die als fehlerfrei betrachtet werden.
- Anzahl fehlerhafter Hosts (**`UnhealthyHostCount`**) – Die Anzahl der Ziel-Instances, die als fehlerhaft betrachtet werden.
- Load Balancer HTTP-4XX (**`HTTPCode_LB_4XX_Count`**) – Anzahl von HTTP-4XX-Client-Fehlercodes, die von Load Balancern verursacht werden. Client-Fehler werden bei Anforderungen mit falschem Format oder unvollständigen Anforderungen generiert. Diese Anforderungen wurden von der Ziel-Instance nicht empfangen. Diese Anzahl umfasst keine Antwortcodes, die von den Ziel-Instances generiert wurden.
- Load Balancer-HTTP-5XX (**`HTTPCode_LB_5XX_Count`**) – Anzahl von HTTP-5XX-Server-Fehlercodes, die von Load Balancern verursacht werden. Hierin sind keine von der Ziel-Instance generierten Antwortcodes enthalten. Die Metrik wird gemeldet, wenn für den Load Balancer keine fehlerfreien Instances angefügt sind oder wenn die Anforderungsrate die Kapazität der Instances (Überlauf) oder des Load Balancers überschreitet.
- HTTP-2XX-Instance (**`HTTPCode_Instance_2XX_Count`**) – Die Anzahl der HTTP-2XX-Antwortcodes, die von den Ziel-Instances generiert werden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.
- HTTP-3XX-Instance (**`HTTPCode_Instance_3XX_Count`**) – Die Anzahl der HTTP-3XX-Antwortcodes, die von den Ziel-Instances generiert werden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.
- HTTP-4XX-Instance (**`HTTPCode_Instance_4XX_Count`**) – Die Anzahl der HTTP-4XX-Antwortcodes, die von den Ziel-Instances generiert werden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.

- HTTP-5XX-Instance (**`HTTPCode_Instance_5XX_Count`**) – Die Anzahl der HTTP-5XX-Antwortcodes, die von den Ziel-Instances generiert werden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.
- Instance-Antwortzeit (**`InstanceResponseTime`**) – Die verstrichene Zeit in Sekunden bis zum Empfang einer Antwort von der Ziel-Instance, nachdem die Anforderung den Load Balancer verlassen hat.
- Anzahl der Anforderungen (**`RequestCount`**) – Die Anzahl von Anforderungen, die über IPv4 verarbeitet wurden. In dieser Zahl sind nur die Anforderungen mit einer Antwort enthalten, die von einer Ziel-Instance des Load Balancers generiert wurden.
- Fehlerzahl-Client-TLS-Vereinbarung (**`ClientTLSNegotiationErrorCount`**) – Die Anzahl der vom Client initiierten TLS-Verbindungen, die keine Sitzung mit de Load Balancer eingerichtet haben, da der Load Balancer einen TLS-Fehler generiert hat. Als mögliche Ursachen kommen unter anderem fehlende Übereinstimmung bei Verschlüsselungsverfahren oder Protokollen infrage.
- Anzahl der abgelehnten Verbindungen (**`RejectedConnectionCount`**) Die Anzahl der abgelehnten Verbindungen, weil der Load Balancer die maximale Anzahl an Verbindungen erreicht hat.

Container-Service-Metriken

Die folgenden Containermetriken sind verfügbar. Weitere Informationen finden Sie unter Anzeigen von Container-Services-Metriken.

- CPU-Nutzung – Der durchschnittliche Prozentsatz der Recheneinheiten, die gegenwärtig auf allen Knoten Ihres Container-Servicess verwendet werden. Diese Metrik gibt die erforderliche Rechenleistung an, um Container-Services auszuführen.
- Speicherauslastung – Der durchschnittliche Prozentsatz des Speichers, der derzeit auf allen Knoten des Container-Servicess verwendet wird. Diese Metrik identifiziert den Speicher, der zum Ausführen von Containern in Ihrem Containerdienst erforderlich ist.

Bucket-Metriken

Die folgenden Metriken sind verfügbar. Weitere Informationen finden Sie unter Anzeigen von Bucket-Metriken.

- Bucket-Größe – Die Menge der in einem Bucket gespeicherten Daten. Zur Berechnung dieses Werts wird die Größe aller (aktuellen und nicht aktuellen) Objekte im Bucket summiert,

einschließlich der Größe aller Teile für sämtliche unvollständigen mehrteiligen Uploads in den Bucket.

- Anzahl Objekte – Die Gesamtzahl der Objekte, die in einem Bucket gespeichert sind. Zur Berechnung dieses Werts werden alle aktuellen und nicht aktuellen Objekte im Bucket sowie die Gesamtanzahl der Teile sämtlicher unvollständiger mehrteiliger Uploads in den Bucket gezählt.

> **Note**
>
> Bucket-Metrikdaten werden nicht gemeldet, wenn Ihr Bucket leer ist.

Themen

Metrikbenachrichtigungen in Lightsail

Sie können Lightsail so konfigurieren, dass Sie benachrichtigt werden, wenn eine Metrik für eine Ihrer Instances, Datenbanken, Load Balancer oder Bereitstellung von Content Delivery Network (CDN) einen angegebenen Schwellenwert überschreitet. Benachrichtigungen können in Form eines Banners, das auf der Lightsail-Konsole angezeigt wird, einer E-Mail an eine von Ihnen angegebene Adresse oder einer SMS-Textnachricht an eine von Ihnen angegebene Mobiltelefonnummer erfolgen.

Um Benachrichtigungen zu erhalten, müssen Sie einen Alarm konfigurieren, der eine Metrik für eine Ihrer Ressourcen überwacht. Sie können beispielsweise einen Alarm konfigurieren, der Sie benachrichtigt, wenn der ausgehende Netzwerkverkehr Ihrer Instance in einer angegebenen Zeitspanne mehr als 500 Kilobyte beträgt. Weitere Informationen finden Sie unter Metrikalarme.

Wenn ein Alarm ausgelöst wird, wird ein Benachrichtigungsbanner in der Lightsail-Konsole angezeigt. Um per E-Mail und SMS benachrichtigt zu werden, müssen Sie in jeder AWS-Region, in der Sie Ihre Ressourcen überwachen möchten, Ihre E-Mail-Adresse und Mobiltelefonnummer

als Benachrichtigungskontakt angeben. Weitere Informationen finden Sie unter Hinzufügen von Benachrichtigungskontakten.

> **Note**
>
> SMS-Textnachrichten werden nicht in allen AWS-Region unterstützt, in denen Sie Lightsail-Ressourcen erstellen können. Außerdem können Textnachrichten in einige Länder und Regionen der Welt nicht gesendet werden. Weitere Informationen finden Sie unter Hinzufügen von Benachrichtigungskontakten.

Wenn Sie wider Erwarten keine Benachrichtigungen erhalten, müssen Sie einige Punkte überprüfen, um sicherzustellen, dass Ihre Benachrichtigungskontakte korrekt konfiguriert sind. Weitere Informationen finden Sie unter Fehlerbehebungs-Benachrichtigungen.

Wenn Sie keine Benachrichtigungen mehr erhalten möchten, können Sie Ihre E-Mail und Ihre Mobiltelefonnummer aus Lightsail entfernen. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen. Sie können einen Alarm auch deaktivieren oder löschen, wenn Sie keine Benachrichtigungen für einen bestimmten Alarm mehr erhalten möchten. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen.

Anzeigen der Burst-Kapazität der Lightsail-Instance

Amazon Lightsail bietet Instances, die eine Basismenge an CPU-Leistung bieten, aber bei Bedarf auch vorübergehend zusätzliche CPU-Leistung über der Basisleistung bereitstellen können. Dies wird als „Bursting“ bezeichnet. Die Basisleistung und die Steigerbarkeit unterliegen den folgenden Instance-Metriken:

- CPU-Auslastung – Prozentsatz der zugeordneten Recheneinheiten, die auf Ihrer Instance verwendet werden. Diese Metrik identifiziert die Verarbeitungsleistung, die zum Ausführen von Anwendungen auf Ihrer Instance verwendet wird.
- CPU-Burst-Kapazität in Prozent – Prozentsatz der CPU-Leistung, die Ihrer Instance zur Verfügung steht.
- CPU-Burst-Kapazität in Minuten – Zeitspanne, die für Ihre Instance zur Steigerung bei 100% CPU-Auslastung verfügbar ist.

In diesem Handbuch zeigen wir Ihnen, wie Sie diese Metriken überwachen, um die Verfügbarkeit Ihrer Instance zu maximieren.

Inhalt

Verstehen der CPU-Basisleistung und Anstiegs der Burst-Kapazität

Lightsail-Instances verdienen kontinuierlich (mit einer Auflösung in Millisekunden) eine festgelegte Rate an CPU-Burst-Kapazität pro Stunde, die auch verbraucht wird, wenn die CPU-Auslastung Ihrer Instance größer als 0 % ist. Der Berechnungsprozess dafür, ob Burst-Kapazität angesammelt oder verbraucht wird, geschieht ebenfalls in Millisekunden. Sie müssen sich also keine Sorgen machen, dass Sie zu viel CPU-Burst-Kapazität verbrauchen; durch eine kurzzeitige CPU-Steigerung wird nur ein Bruchteil der Burst-Kapazität verbraucht.

Wenn Ihre Instance weniger CPU-Ressourcen benötigt als für die Basisleistung erforderlich ist (z. B. wenn sie im Leerlauf ist), wird die nicht verbrauchte CPU-Burst-Kapazität in Prozent und Minuten angesammelt. Benötigt Ihre Instance eine höhere als die Basisleistung, verbraucht sie die angesammelte CPU-Burst-Kapazität. Je mehr CPU-Burst-Kapazität sich für Ihre Instance angesammelt hat, desto länger kann die Leistung über die Basisleistung hinaus gesteigert werden, wenn mehr Leistung benötigt wird.

Basisleistung (CPU)

In der folgenden Liste sind die Leistungsgrundlagen für jeden Lightsail-Instance-Plan aufgeführt:

- Die Instance-Tarife Linux oder Unix 3,50 USD/Monat und Windows 8 USD/Monat (2 vCPU, 512 MB Arbeitsspeicher, 30 GB Speicher) beinhalten eine Leistung-Baseline von 5 % für CPU-Auslastung.
- Die Instance-Tarife Linux oder Unix 5 USD/Monat und Windows 12 USD/Monat (2 vCPU, 1 GB Arbeitsspeicher, 40 GB Speicher) beinhalten eine Leistung-Baseline von 10 % für CPU-Auslastung.
- Die Instance-Tarife Linux oder Unix 10 USD/Monat und Windows 20 USD/Monat (2 vCPU, 2 GB Arbeitsspeicher, 60 GB Speicher) beinhalten eine Leistung-Baseline von 20 % für CPU-Auslastung.
- Die Instance-Tarife Linux oder Unix 20 USD/Monat und Windows 40 USD/Monat (2 vCPU, 4 GB Arbeitsspeicher, 80 GB Speicher) beinhalten eine Leistung-Baseline von 20 % für CPU-Auslastung.

- Die Instance-Tarife Linux oder Unix 40 USD/Monat und Windows 70 USD/Monat (2 vCPU, 8 GB Arbeitsspeicher, 160 GB Speicher) beinhalten eine Leistung-Baseline von 30 % für CPU-Auslastung.
- Die Instance-Tarife Linux oder Unix 80 USD/Monat und Windows 120 USD/Monat (4 vCPU, 16 GB Arbeitsspeicher, 320 GB Speicher) beinhalten eine Leistung-Baseline von 40 % für CPU-Auslastung.
- Die Instance-Tarife Linux oder Unix 160 USD/Monat und Windows 240 USD/Monat (8 vCPU, 32 GB Arbeitsspeicher, 640 GB Speicher) beinhalten eine Leistung-Baseline von 40 % für CPU-Auslastung.

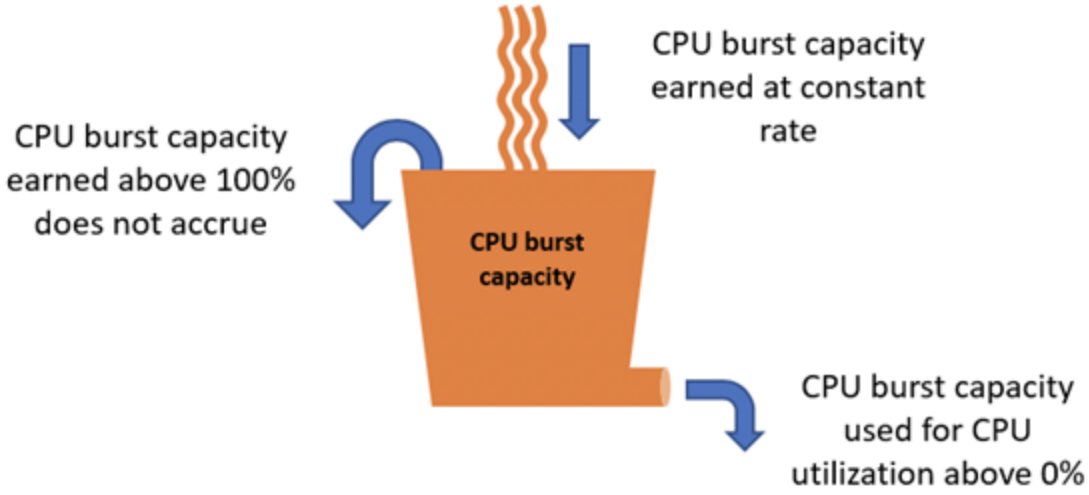
Diese Basisleistungen gelten pro vCPU. Das Metrikdiagramm zur CPU-Auslastung in der Lightsail-Konsole mittelt die CPU-Auslastung und die Baseline für Instances mit mehr als einer vCPU. Beispielsweise verfügt eine Instance für 40 USD/Monat über zwei vCPUs und einer durchschnittlichen CPU-Basisauslastung von 30 %. Daher gilt, wenn:

- Eine vCPU mit 50% und die andere mit 0% arbeitet, wird im Diagramm eine durchschnittliche CPU-Auslastung von 25% angezeigt. Dadurch wird die CPU-Auslastung der Instance unter die 30%-Baseline und in die nachhaltige Zone gesetzt.
- Eine vCPU mit 30% und die andere mit 20% arbeitet, wird im Diagramm eine durchschnittliche CPU-Auslastung von 25% angezeigt. Dadurch wird die CPU-Auslastung der Instance unter die 30%-Baseline und in die nachhaltige Zone gesetzt.
- Eine vCPU mit 35% und die andere mit 25% arbeitet, wird im Diagramm eine durchschnittliche CPU-Auslastung von 30% angezeigt. Dadurch wird die CPU-Auslastung der Instance auf die 30%-Baseline gesetzt.
- Eine vCPU mit 100% und die andere mit 90% arbeitet, wird im Diagramm eine durchschnittliche CPU-Auslastung von 95% angezeigt. Dadurch wird die CPU-Auslastung der Instance über die 30%-Baseline und in die burstfähige Zone gesetzt.

> **Note**
>
> Weitere Informationen zu den nachhaltigen und burstfähigen Zonen finden Sie unter Identifizieren, wann Ihre Instance gesteigert wird weiter unten in diesem Leitfaden.

Ansammlung der CPU-Burst-Kapazität

Alle Lightsail-Instance-Pläne sammeln 4,17 % der CPU-Burst-Kapazität pro Stunde an. Die CPU-Burst-Kapazität in Prozent, die angesammelt werden kann, entspricht der CPU-Burst-Kapazität in Prozent, die in einem 24-Stunden-Zeitraum erzielt werden kann. Ihre Instance stoppt die CPU-Burst-Kapazität in Prozent anzusammeln, wenn sie 100% erreicht.



Important

Aufgelaufene CPU-Burst-Kapazität

- Instances, die vor dem 29. Juni 2023 erstellt wurden – CPU-Burst-Kapazität bleibt nicht erhalten, wenn Ihre Instance gestoppt wird. Wenn Sie Ihre Instance anhalten, verliert sie die gesamte angesammelte Burst-Kapazität.
- Instances, die am oder nach dem 29. Juni 2023 erstellt wurden – Die CPU-Burst-Kapazität bleibt sieben Tage lang zwischen dem Anhalten und Starten der Instance bestehen.
- Angesammelte CPU-Burst-Kapazität auf einer laufenden Instance verfällt nicht.

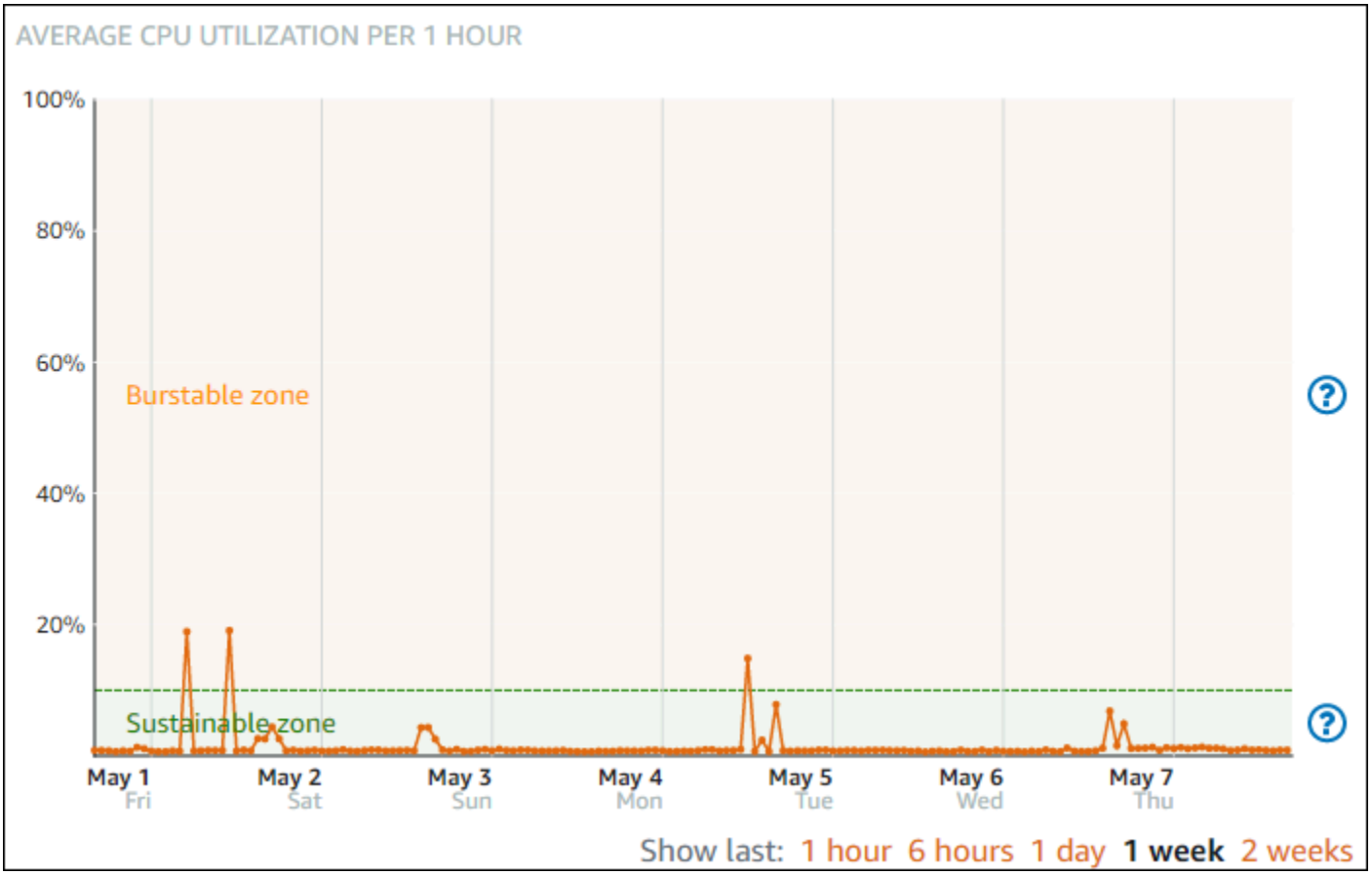
Lightsail-Instances erhalten zusätzliche CPU-Burst-Kapazität beim Start. Dies wird als Start-CPU-Burst-Kapazität bezeichnet. Mit der CPU-Burst-Startkapazität können Instances sofort nach dem Start gesteigert werden, bevor sie zusätzliche Burst-Kapazität angesammelt haben. Die CPU-Burst-Startkapazität wird nicht auf das Limit der Burst-Kapazität angerechnet. Wenn Ihre Instance ihre CPU-Burst-Startkapazität nicht verbraucht hat und über einen Zeitraum von 24 Stunden im Leerlauf

bleibt und gleichzeitig mehr Burst-Kapazität ansammelt, wird ihr Metrikdiagramm für die CPU-Burst-Kapazität (Prozentsatz) als mehr als 100% angezeigt.

Darüber hinaus starten einige Lightsail-Instances im Startmodus, wodurch vorübergehend einige der Leistungsbeschränkungen entfernt werden, die normalerweise bei Burstable-Instances bestehen. Mit dem Startmodus können Sie ressourcenintensive Skripte beim Start ausführen, ohne die Gesamtleistung Ihrer Instance zu beeinträchtigen.

Identifizieren, wann Ihre Instance gesteigert wird

Das Diagramm der CPU-Auslastungsmetrik für Ihre Instances enthält eine nachhaltige Zone und eine burstfähige Zone. Im folgenden Beispiel für das Metrikdiagramm der CPU-Auslastung beträgt die Basisleistung 10 %, da die Instance den Instance-Tarif für 5 USD/Monat verwendet.



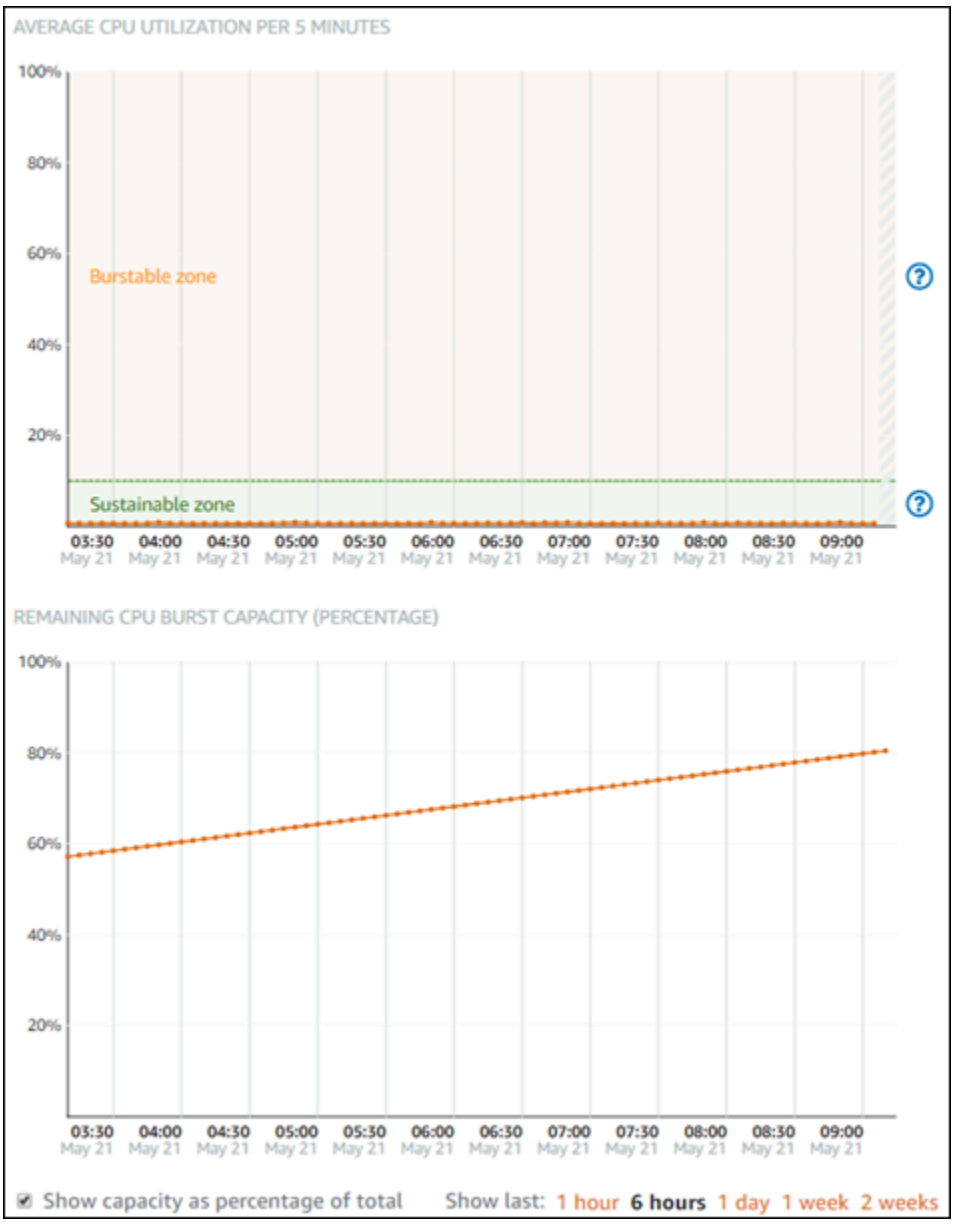
Ihre Lightsail-Instance kann unbegrenzt in der nachhaltigen Zone arbeiten, ohne dass dies Auswirkungen auf den Betrieb Ihres Systems hat. Ihre Instance kann den Betrieb in der burstfähigen Zone beginnen, wenn sie unter hoher Last steht, z. B. beim Kompilieren von Code, beim Installieren neuer Software, beim Ausführen eines Stapelverarbeitungsauftrags (Batch-Job) oder beim Bewältigen von Spitzenlastanforderungen. Bei Betrieb in der burstfähigen Zone ruft Ihre Instance

eine höhere Anzahl von CPU-Zyklen ab. Daher kann sie nur begrenzte Zeit in dieser Zone betrieben werden.

Der Zeitraum, in dem Ihre Instance in der burstfähigen Zone betrieben werden kann, hängt davon ab, wie weit sie sich in der burstfähigen Zone befindet. Eine Instance, die am unteren Ende der burstfähigen Zone operiert, kann länger betrieben werden als eine Instance, die am oberen Ende der burstfähigen Zone operiert. Eine Instance, die sich für einen längeren Zeitraum an einer beliebigen Stelle in der burstfähigen Zone befindet, verbraucht jedoch letztlich die gesamte CPU-Kapazität, bis sie wieder in der nachhaltigen Zone betrieben wird. Daher ist es wichtig, auch die verbleibende CPU-Burst-Kapazität zu überwachen, was im folgenden Abschnitt dieses Handbuchs beschrieben wird.

Überwachung der CPU-Burst-Kapazität

Auf der Seite CPU-Übersicht in der Lightsail-Konsole wird die CPU-Auslastung Ihrer Instance im Vergleich zur verfügbaren CPU-Burst-Kapazität angezeigt. Im folgenden CPU-Übersichtsbeispiel ist der Prozentsatz der CPU-Burst-Kapazität gestiegen, da die Instance kontinuierlich unter ihrer Baseline in der nachhaltigen Zone betrieben wurde.



Die Diagrammansicht der verbleibenden CPU-Burst-Kapazität kann zwischen Prozent und Minuten der CPU-Burst-Kapazität umgeschaltet werden. Ihre Instance verbraucht mehr CPU-Burst-Kapazität, wenn sie in der burstfähigen Zone betrieben wird. Die Metrik „CPU-Burst-Kapazität in Minuten“ ist die Zeitspanne, die für Ihre Instance zur Steigerung bei 100% CPU-Auslastung verfügbar ist. Sie wird mit der gleichen Rate verbraucht wie die aktuelle Instance-CPU-Auslastung in Prozent, wenn Sie in der burstfähigen Zone arbeiten. Beispielsweise verfügt eine Instance für 5 USD/Monat über eine CPU-Basisauslastung von 10 % und sammelt sechs Minuten an Minuten der CPU-Burst-Kapazität pro Stunde an. Arbeitet die Instance daher bei:

- 100% CPU-Auslastung in der burstfähigen Zone für einen Zeitraum von 60 Minuten, dann verbraucht sie die Minuten der CPU-Burst-Kapazität mit einer Rate von 100% in diesem Zeitraum.

Die Instance verbraucht 60 Minuten CPU-Burst-Kapazität und sammelt sechs Minuten für einen Gesamtverbrauch von 54 Minuten an.

- 50% CPU-Auslastung in der burstfähigen Zone für einen Zeitraum von 60 Minuten, dann verbraucht sie die Minuten der CPU-Burst-Kapazität mit einer Rate von 50% in diesem Zeitraum. Die Instance verbraucht 30 Minuten CPU-Burst-Kapazität und sammelt sechs Minuten für einen Gesamtverbrauch von 24 Minuten an.
- 10% CPU-Auslastung auf der Baseline-Stufe der Instance für einen Zeitraum von 60 Minuten, dann verbraucht sie die Minuten der CPU-Burst-Kapazität mit einer Rate von 10% in diesem Zeitraum. Die Instance verbraucht 6 Minuten CPU-Burst-Kapazität und sammelt 6 Minuten an. Wenn eine Instance auf ihrer Baseline-Stufe arbeitet, erhöhen oder verringern sich die Minuten der CPU-Burst-Kapazität nicht.
- 5% CPU-Auslastung in der nachhaltigen Zone für einen Zeitraum von 60 Minuten, dann verbraucht sie die Minuten der CPU-Burst-Kapazität mit einer Rate von 5% in diesem Zeitraum. Die Instance verbraucht drei Minuten CPU-Burst-Kapazität und sammelt 6 Minuten für eine Nettoansammlung von drei Minuten an.

Alternativ kann die Instance, wenn sie 60 Minuten CPU-Burst-Kapazität angesammelt hat, 60 Minuten lang bei 100% CPU-Auslastung, 120 Minuten bei 50% oder 150 Minuten bei 25% betrieben werden.

Fehlerbehebung von hoher CPU-Auslastung

Ihre Instance verwendet die gesamte Burst-Kapazität, wenn sie häufig oder über längere Zeiträume in der burstfähigen Zone arbeitet. Dies kann bedeuten, dass Ihre Instance unterdimensioniert ist. Es kann auch sein, dass ein Service zu häufig ausgeführt wird oder Ihre Instance unnötige Software ausführt.

Untersuchen Sie mithilfe von Tools wie top auf Linux/Unix-Instances und Task-Manager auf Windows Server-Instances, was dazu führt, dass Ihre Instance gesteigert wird. Diese Tools zeigen Ihnen die Services an, die Ressourcen in Ihrer Instance verbrauchen. Bestimmen Sie, welche Services die meisten Ressourcen verbrauchen, und ermitteln Sie, ob sie deaktiviert werden können, ohne die Workload Ihrer Instance zu beeinträchtigen. Durch Deaktivieren von Services oder Deinstallation von Software können Sie möglicherweise die Steigerung Ihrer Instance verringern und vermeiden, dass Sie Ihre Instance vergrößern müssen.

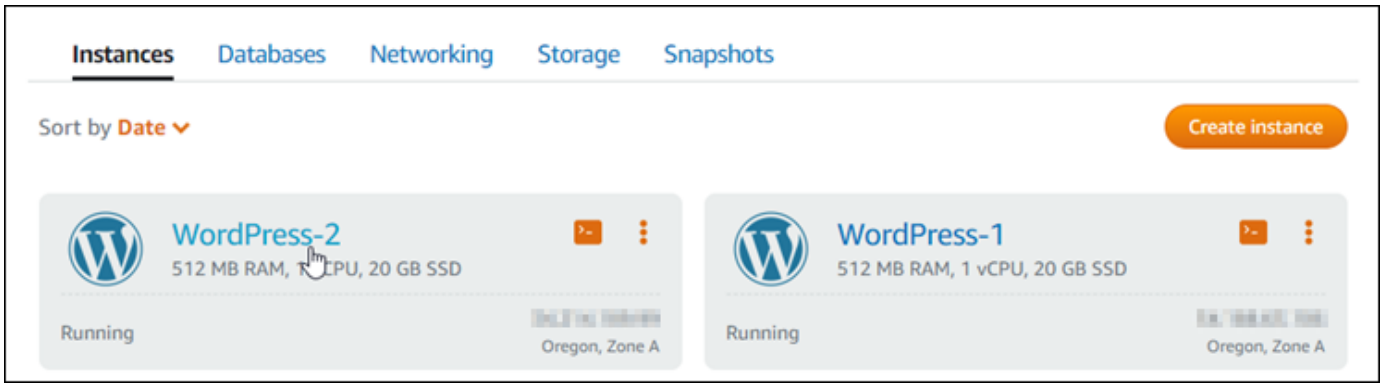
Wenn Ihre Instance wirklich unterdimensioniert ist und Sie die CPU-Auslastung nicht senken können, können Sie den Burst-Kapazitätsverbrauch reduzieren, indem Sie mehr Rechenleistung hinzufügen. Dazu erstellen Sie einen Snapshot Ihrer Instance und anschließend eine neue Instance aus dem

Snapshot mit einem größeren Lightsail-Instance-Plan. Verwenden Sie beispielsweise den Tarif 20 USD pro Monat für Ihre neue Instance anstelle des für die vorherige Instance verwendeten Tarifs von 10 USD pro Monat. Wenn Ihre neue Instance ausgeführt wird, nehmen Sie bei Bedarf Änderungen am DNS Ihrer Arbeitslast vor, um die alte Instance durch die neue zu tauschen. Löschen Sie Ihre alte unterdimensionierte Instance, nachdem der Datenverkehr an Ihre neue Instance weitergeleitet wird. Weitere Informationen finden Sie unter Snapshots.

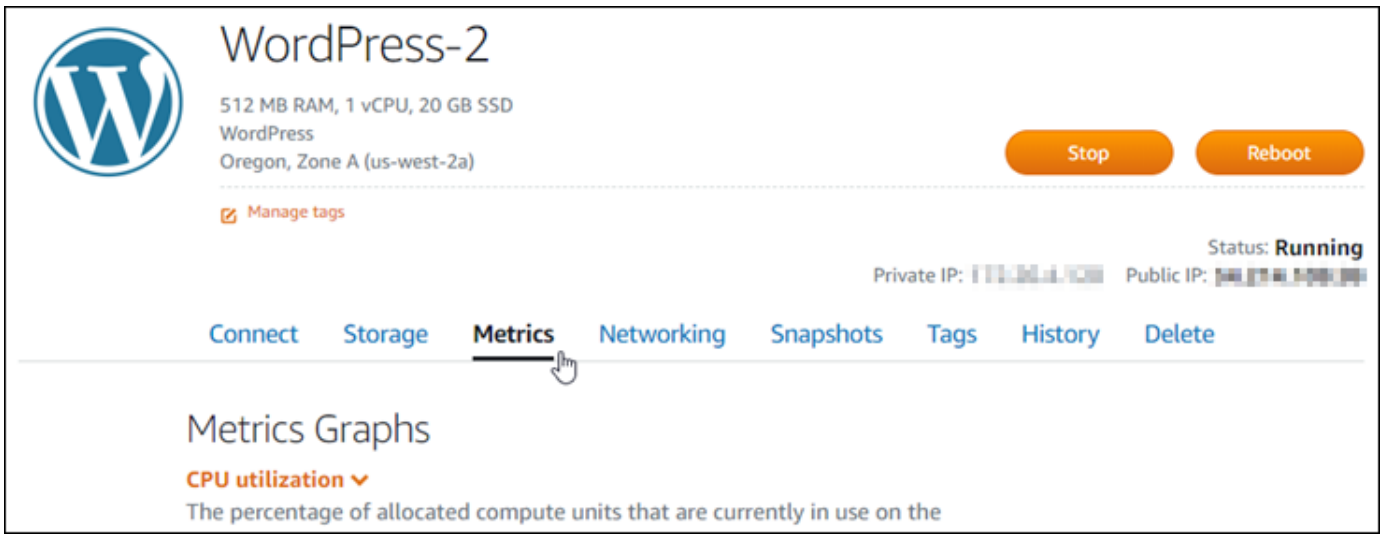
Anzeigen der Instance-Burst-Kapazität

Führen Sie die folgenden Schritte aus, um auf die CPU-Übersichtsseite zuzugreifen und die CPU-Auslastung Ihrer Instance und die verbleibende CPU-Burst-Kapazität anzuzeigen.

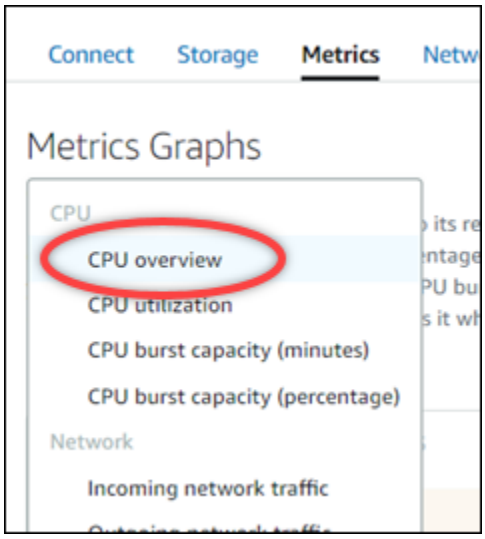
1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Instances aus.
3. Wählen Sie den Namen der Instance aus, für die Sie die CPU-Auslastung und die Burst-Kapazität anzeigen möchten.



4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Seite der Instance-Verwaltung aus.



5. Wählen Sie CPU-Überblick im Dropdown-Menü unter dem Titel Metriken grafisch darstellen.



Auf der Seite werden die Diagramme Durchschnittliche CPU-Auslastung per 5 Minuten und Verbleibenden CPU-Burst-Kapazität angezeigt.

> **Note**
>
> Das Diagramm Verbleibende CPU-Burst-Kapazität zeigt möglicherweise eine Zone Launch mode (Startmodus) für einen Augenblick, nachdem Sie eine Instance erstellt haben. Einige Lightsail-Instances starten im Startmodus, wodurch vorübergehend einige der Leistungsbeschränkungen entfernt werden, die normalerweise bei Burstable-Instances bestehen. Mit dem Startmodus können Sie ressourcenintensive Skripte beim Start ausführen, ohne die Gesamtleistung Ihrer Instance zu beeinträchtigen.

6. In den Metrikdiagrammen können Sie die folgenden Aktionen ausführen:

   - Wählen Sie für das Diagramm „Burst-Kapazität“ die Option Kapazität als Prozentsatz der Summe anzeigen aus, um die Ansicht von verfügbarer Burst-Kapazität in Minuten in verfügbarer Burst-Kapazität in Prozent zu ändern.
   - Sie können die Ansicht des Diagramms ändern, um Daten für 1 Stunde, 6 Stunden, 1 Tag, 1 Woche und 2 Wochen anzuzeigen.
   - Sie können den Cursor auf einem Datenpunkt anhalten, um detaillierte Informationen zu diesem Datenpunkt anzuzeigen.

- Fügen Sie einen Alarm hinzu, der Sie benachrichtigt, wenn die CPU-Auslastung und Burst-Kapazität einen von Ihnen festgelegten Schwellenwert überschreitet. Alarme können nicht auf der CPU-Übersichtsseite hinzugefügt werden. Sie müssen sie in den einzelnen Metrik-Diagrammseiten der CPU-Auslastung, der CPU-Burst-Kapazität in Prozent und der CPU-Burst-Kapazität in Minuten hinzufügen. Weitere Informationen finden Sie unter Alarme und Erstellen von Instance-Metrikalarmen.

Anzeigen von Lightsail-Instance-Metriken

Nachdem Sie eine Instance in Amazon Lightsail gestartet haben, können Sie ihre Metrikdiagramme auf der Registerkarte Metrics (Metriken) der Verwaltungsseite der Instance anzeigen. Die Überwachung von Metriken ist ein wichtiger Teil, um die Zuverlässigkeit, Verfügbarkeit und Performance Ihrer Ressourcen aufrechtzuerhalten. Überwachen und sammeln Sie regelmäßig Metrikdaten von Ihren Ressourcen, damit Sie bei Auftreten eines Mehrpunkt-Fehlers diesen leichter debuggen können. Weitere Informationen zu Metriken finden Sie unter Metriken in Amazon Lightsail.

Bei der Überwachung Ihrer Ressourcen sollten Sie einen Bereich für die normale Ressourcenleistung in Ihrer Umgebung festlegen. Anschließend können Sie Alarme in der Lightsail-Konsole konfigurieren, damit Sie benachrichtigt werden, wenn die Leistung Ihrer Ressourcen außerhalb der angegebenen Schwellenwerte liegt. Weitere Informationen finden Sie unter Benachrichtigungen und Alarme.

Inhalt

Verfügbare Instance-Metriken

Die folgenden Instance-Metriken sind verfügbar:

- CPU-Auslastung (**`CPUUtilization`**) – Der Prozentsatz der zugeordneten Recheneinheiten, die derzeit auf der Instance verwendet werden. Diese Metrik identifiziert die Verarbeitungsleistung für die Ausführung der Anwendungen auf der Instance. Die Tools Ihres Betriebssystems können geringere Prozentsätze als Lightsail anzeigen, wenn der Instance kein vollständiger Prozessorkern zugeordnet ist.

Wenn Sie die Metrik-Diagramme für die CPU-Auslastung für Ihre Instances in der Lightsail-Konsole anzeigen, werden nachhaltige und burstfähige Zonen angezeigt. Weitere Informationen zur Bedeutung dieser Zonen finden Sie unter CPU-Auslastung in nachhaltigen und burstfähigen Zonen.

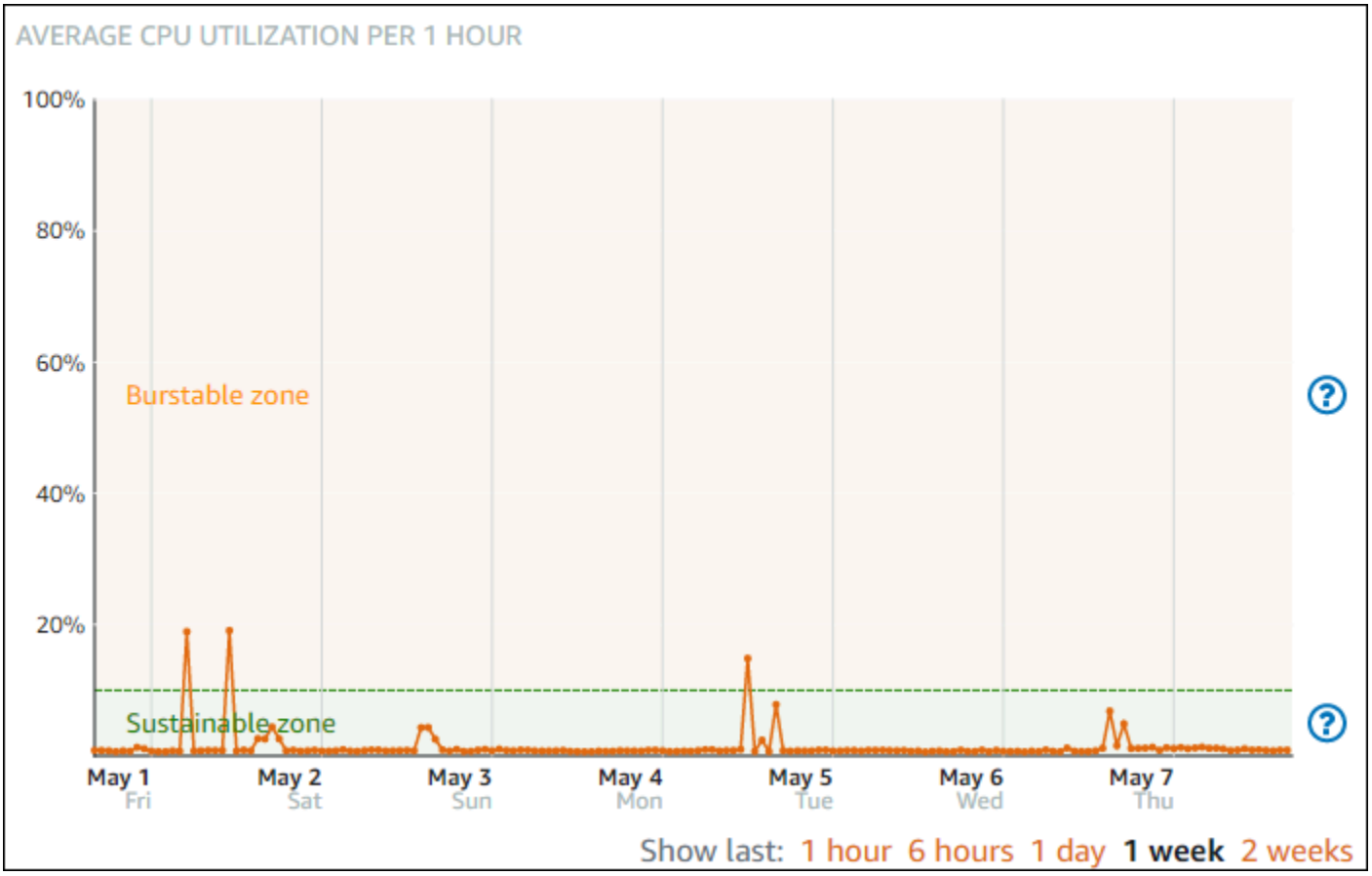
- Burst-Kapazitätsminuten (**`BurstCapacityTime`**) und Prozentsatz (**`BurstCapacityPercentage`**) – Burst-Kapazitätsminuten stellen die Zeit dar, die Ihrer Instance für das Bursten bei 100 % CPU-Auslastung zur Verfügung steht. Der Prozentsatz der Burst-Kapazität ist der Prozentsatz der CPU-Leistung, die Ihrer Instance zur Verfügung steht. Ihre Instance verbraucht kontinuierlich Burst-Kapazität und sammelt diese an. Die Burst-Kapazitätsminuten werden nur dann mit voller Geschwindigkeit verbraucht, wenn Ihre Instance mit 100 % CPU-Auslastung arbeitet. Weitere Informationen zur Instance-Burst-Kapazität finden Sie unter Anzeigen von Instance-Burst-Kapazität.
- Eingehender Netzwerkdatenverkehr (**`NetworkIn`**) – Die Anzahl der Bytes, die von der Instance an allen Netzwerkschnittstellen empfangen wurde. Diese Metrik gibt das eingehende Netzwerkdatenvolumen an der Instance an. Der ermittelte Wert ist die Anzahl der während des Zeitraums empfangenen Byte. Da diese Metrik in 5-Minuten-Intervallen gemeldet wird, teilen Sie die gemeldete Zahl durch 300, um Byte/Sekunde zu erhalten.
- Ausgehender Netzwerkdatenverkehr (**`NetworkOut`**) – Die Anzahl der Bytes, die von der Instance an allen Netzwerkschnittstellen versandt wurde. Diese Metrik gibt das ausgehende Netzwerkdatenvolumen an einer Instance an. Der ermittelte Wert ist die Anzahl der während des Zeitraums gesendeten Bytes. Da diese Metrik in 5-Minuten-Intervallen gemeldet wird, teilen Sie die gemeldete Zahl durch 300, um Byte/Sekunde zu erhalten.
- Fehler bei der Zustandsprüfung (**`StatusCheckFailed`**) – Berichtet, ob die Instance sowohl die Instance-Statusprüfung als auch die System-Statusprüfung bestanden hat oder nicht. Diese Metrik nimmt den Wert 0 (bestanden) oder 1 (fehlgeschlagen) an. Diese Metrik ist mit einer einminütigen Frequenz verfügbar.
- Fehler bei der Instance-Statusprüfung (**`StatusCheckFailed_Instance`**) – Berichtet, ob die Instance die Instance-Statusprüfung bestanden hat oder nicht. Diese Metrik nimmt den Wert 0 (bestanden) oder 1 (fehlgeschlagen) an. Diese Metrik ist mit einer einminütigen Frequenz verfügbar.
- Fehler bei der System-Statusprüfung (**`StatusCheckFailed_System`**) – Berichtet, ob die Instance die System-Statusprüfung bestanden hat oder nicht. Diese Metrik nimmt den Wert 0 (bestanden) oder 1 (fehlgeschlagen) an. Diese Metrik ist mit einer einminütigen Frequenz verfügbar.

- Keine Token-Metadatenanforderungen (**`MetadataNoToken`**) – Gibt an, wie oft erfolgreich ohne Token auf den Instance-Metadatenservice zugegriffen wurde. Diese Metrik bestimmt, ob Prozesse vorhanden sind, die mit Instance-Metadatenservice Version 1, das keinen Token verwendet, auf Instance-Metadaten zugreifen. Wenn alle Anfragen Token-gestützte Sitzungen verwenden, d. h. Instance-Metadatenservice Version 2, ist der Wert 0. Weitere Informationen finden Sie unter Instance-Metadaten und Benutzerdaten.

Nachhaltige und burstfähige Zonen der CPU-Auslastung

Lightsail verwendet burstfähige Instances (zu Spitzenlastleistung fähige Instances, sog. „Burstable Instances“), die neben einer CPU-Basisleistung auch vorübergehend zusätzliche CPU-Leistung über die Basisleistung hinaus bereitstellen können. Dies wird als „Bursting“ bezeichnet. Bei burstfähigen Instances müssen Sie für Ihre Instance keine Überkapazität bereitstellen, um gelegentliche Lastspitzen zu bewältigen, sodass Sie nicht für Kapazitäten bezahlen müssen, die Sie nie nutzen.

Das Diagramm der CPU-Auslastungsmetrik für Ihre Instances enthält eine nachhaltige Zone und eine burstfähige Zone. Ihre Lightsail-Instance kann unbegrenzt in der nachhaltigen Zone arbeiten, ohne dass dies Auswirkungen auf den Betrieb Ihres Systems hat.



Ihre Instance kann den Betrieb in der burstfähigen Zone beginnen, wenn sie unter hoher Last steht, z. B. beim Kompilieren von Code, beim Installieren neuer Software, beim Ausführen eines Stapelverarbeitungsauftrags (Batch-Job) oder beim Bewältigen von Spitzenlastanforderungen. Bei Betrieb in der burstfähigen Zone ruft Ihre Instance eine höhere Anzahl von CPU-Zyklen ab. Daher kann sie nur begrenzte Zeit in dieser Zone betrieben werden.

Der Zeitraum, in dem Ihre Instance in der burstfähigen Zone betrieben werden kann, hängt davon ab, wie weit sie sich in der burstfähigen Zone befindet. Eine Instance, die am unteren Ende der burstfähigen Zone operiert, kann länger betrieben werden als eine Instance, die am oberen Ende der burstfähigen Zone operiert. Eine Instance, die sich für einen längeren Zeitraum an einer beliebigen Stelle in der burstfähigen Zone befindet, verbraucht jedoch letztlich die gesamte CPU-Kapazität, bis sie wieder in der nachhaltigen Zone betrieben wird.

Überwachen Sie die CPU-Auslastungsmetrik Ihrer Instance, um zu sehen, wie ihre Leistung zwischen den nachhaltigen und burstfähigen Zonen verteilt wird. Wenn Ihr System nur gelegentlich in die burstfähige Zone wechselt, sollten Sie die Instance, die Sie ausführen, weiterhin verwenden. Wenn Sie jedoch sehen, dass Ihre Instance viel Zeit in der burstfähigen Zone verbringt, sollten Sie möglicherweise zu einem höheren Tarif für Ihre Instance wechseln (z. B. Tarif für 10 USD/Monat anstelle des Tarifs für 3,50 USD/Monat). Sie können zu einem höheren Tarif wechseln, indem Sie einen neuen Snapshot Ihrer Instance erstellen und dann eine neue Instance aus dem Snapshot erstellen.

Anzeigen von Instance-Metriken in der Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um Instance-Metriken in der Lightsail-Konsole anzuzeigen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Instances.
3. Wählen Sie den Namen der Instance aus, für die Sie Metriken anzeigen möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Seite der Instance-Verwaltung aus.
5. Wählen Sie die Metrik aus, die Sie im Dropdown-Menü unter der Überschrift Metrics graphs (Metrikdiagramme) anzeigen möchten.

   Das Diagramm zeigt eine visuelle Darstellung der Datenpunkte für die gewählte Metrik an.

> **Note**
>
> Wenn Sie die Metrik-Diagramme für die CPU-Auslastung für Ihre Instances in der Lightsail-Konsole anzeigen, werden nachhaltige und burstfähige Zonen angezeigt. Weitere Informationen zu diesen Zonen finden Sie unter CPU-Auslastung in nachhaltigen und burstfähigen Zonen.

6. Im Metrikdiagramm können Sie die folgenden Aktionen ausführen:

   - Sie können die Ansicht des Diagramms ändern, um Daten für 1 Stunde, 6 Stunden, 1 Tag, 1 Woche und 2 Wochen anzuzeigen.
   - Sie können den Cursor auf einem Datenpunkt anhalten, um detaillierte Informationen zu diesem Datenpunkt anzuzeigen.
   - Sie können einen Alarm für die ausgewählte Metrik hinzufügen, damit Sie benachrichtigt werden, wenn die Metrik einen von Ihnen angegebenen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Alarme und Erstellen von Instance-Metrikalarmen.

Nächste Schritte

Es gibt einige zusätzliche Aufgaben, die Sie für Ihre Instance-Metriken ausführen können:

- Sie können einen Alarm für die ausgewählte Metrik hinzufügen, damit Sie benachrichtigt werden, wenn die Metrik einen von Ihnen angegebenen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Metrikalarme und Erstellen von Instance-Metrikalarmen.
- Wenn ein Alarm ausgelöst wird, wird ein Benachrichtigungsbanner in der Lightsail-Konsole angezeigt. Um per E-Mail und SMS benachrichtigt zu werden, müssen Sie in jeder AWS-Region, in der Sie Ihre Ressourcen überwachen möchten, Ihre E-Mail-Adresse und Mobiltelefonnummer als Benachrichtigungskontakt angeben. Weitere Informationen finden Sie unter Hinzufügen von Benachrichtigungskontakten.
- Wenn Sie keine Benachrichtigungen mehr erhalten möchten, können Sie Ihre E-Mail und Ihre Mobiltelefonnummer aus Lightsail entfernen. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen. Sie können einen Alarm auch deaktivieren oder löschen, wenn Sie keine Benachrichtigungen für einen bestimmten Alarm mehr erhalten möchten. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen.

Metrikalarme in Lightsail

Sie können in Amazon Lightsail einen Alarm erstellen, der eine einzelne Metrik für Ihre Instances, Datenbanken, Load Balancers und Verteilungen von Netzwerken für die Bereitstellung von Inhalten (Content Delivery Network, CDN) überwacht. Der Alarm kann so konfiguriert werden, dass Sie basierend auf dem Wert der Metrik relativ zu einem von Ihnen angegebenen Schwellenwert benachrichtigt werden. Benachrichtigungen können ein in der Lightsail-Konsole angezeigtes Banner, eine an Ihre E-Mail-Adresse gesendete E-Mail oder eine an Ihre Mobiltelefonnummer gesendete SMS-Nachricht sein. In diesem Handbuch beschreiben wir die Alarmbedingungen und Einstellungen, die Sie konfigurieren können.

Inhalt

Konfigurieren eines Alarms

Um einen Alarm in der Lightsail-Konsole hinzuzufügen, navigieren Sie zur Registerkarte Metrics (Metriken) Ihrer Instance, Ihrer Datenbank, Ihrer Load Balancers oder Ihrer CDN-Verteilung. Wählen Sie dann die Metrik aus, die Sie überwachen möchten, und wählen Sie Add alarm (Alarm hinzufügen). Sie können zwei Alarme pro Metrik hinzufügen. Weitere Informationen zu Metriken erhalten Sie unter Ressourcenmetriken.

Um den Alarm zu konfigurieren, identifizieren Sie zunächst einen Schwellenwert, bei dem es sich um den Metrikwert handelt, an dem sich der Alarmzustand ändert (z. B. Wechsel vom Zustand `OK` in den Zustand `ALARM` oder umgekehrt). Weitere Informationen finden Sie unter Alarmszustände. Wählen Sie dann einen Vergleichsoperator aus, der verwendet wird, um die Metrik mit dem Schwellenwert zu vergleichen. Die verfügbaren Operatoren sind greater than or equal to (größer als oder gleich), greater than (größer als), less than (kleiner als) und less than or equal to (kleiner als oder gleich).

Anschließend geben Sie an, wie oft der Schwellenwert überschritten werden muss und wie lange die Metrik ausgewertet wird, damit über den Alarm der Status geändert wird. Lightsail wertet alle 5 Minuten Datenpunkte für Alarme aus, wobei jeder Datenpunkt einen 5-minütigen Zeitraum aggregierter Daten darstellt. Beispiel: Wenn Sie angeben, dass der Alarm ausgelöst werden soll, wenn der Schwellenwert 2 Mal überschritten wird, muss der Bewertungszeitraum in den letzten 10 Minuten oder größer (bis zu 24 Stunden) sein. Wenn Sie angeben, dass der Alarm ausgelöst werden soll, wenn der Schwellenwert 10 Mal überschritten wird, muss der Bewertungszeitraum in den letzten 50 Minuten oder größer (bis zu 24 Stunden) sein.

Nach dem Konfigurieren der Bedingungen für den Alarm können Sie festlegen, wie Sie benachrichtigt werden möchten. Benachrichtigungsbanner werden immer in der Lightsail-Konsole angezeigt, wenn der Alarm aus dem Zustand `OK` in den Zustand `ALARM` wechselt. Sie können sich auch per E-Mail und SMS-Textnachricht benachrichtigen lassen, müssen aber Benachrichtigungskontakte dafür konfigurieren. Weitere Informationen finden Sie unter Metrik-Benachrichtigungen. Wenn Sie sich per E-Mail und/oder SMS-Textnachricht benachrichtigen lassen, können Sie sich auch benachrichtigen lassen, wenn sich der Alarmzustand von `ALARM` in `OK` ändert. Dies wird als Entwarnung bezeichnet.

In Advanced settings (Erweiterte Einstellungen) für den Alarm können Sie festlegen, wie Lightsail mit fehlenden Metrikdaten umgeht. Weitere Informationen finden Sie unter Konfigurieren der Behandlung fehlender Daten durch Alarme.

Alarmzustände

Ein Alarm befindet sich immer in einem der folgenden Zustände:

- ALARM – Die Metrik liegt außerhalb des festgelegten Schwellenwerts.

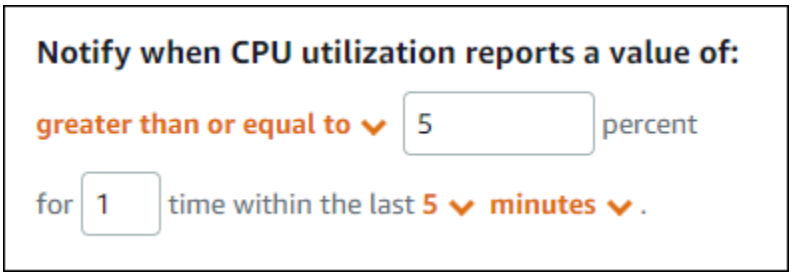
  Wenn Sie beispielsweise den Vergleichsoperator greater than (größer als) auswählen, befindet sich der Alarm im Zustand `ALARM`, wenn die Metrik größer als der festgelegte Schwellenwert ist. Wenn Sie den Vergleichsoperator less than (weniger als) auswählen, befindet sich der Alarm im Zustand `ALARM`, wenn die Metrik kleiner als der festgelegte Schwellenwert ist.
- OK – Die Metrik liegt innerhalb des festgelegten Schwellenwerts.

  Wenn Sie beispielsweise den Vergleichsoperator greater than (größer als) auswählen, befindet sich der Alarm im Zustand `OK`, wenn die Metrik kleiner als der festgelegte Schwellenwert ist. Wenn Sie den Vergleichsoperator less than (weniger als) auswählen, befindet sich der Alarm im Zustand `OK`, wenn die Metrik größer als der festgelegte Schwellenwert ist.
- INSUFFICIENT_DATA – Der Alarm wurde soeben erst gestartet; die Metrik ist nicht verfügbar oder es sind nicht genügend Metrik-Daten verfügbar, um den Alarmstatus zu bestimmen.

Alarme werden nur für Statusänderungen ausgelöst. Alarme werden nicht einfach ausgelöst, weil sie sich in einem bestimmten Zustand befinden – der Zustand muss sich geändert haben. Wenn ein Alarm ausgelöst wird, wird ein Banner in der Lightsail-Konsole angezeigt. Sie können Alarme auch so konfigurieren, dass Sie per E-Mail und SMS-Textnachricht benachrichtigt werden.

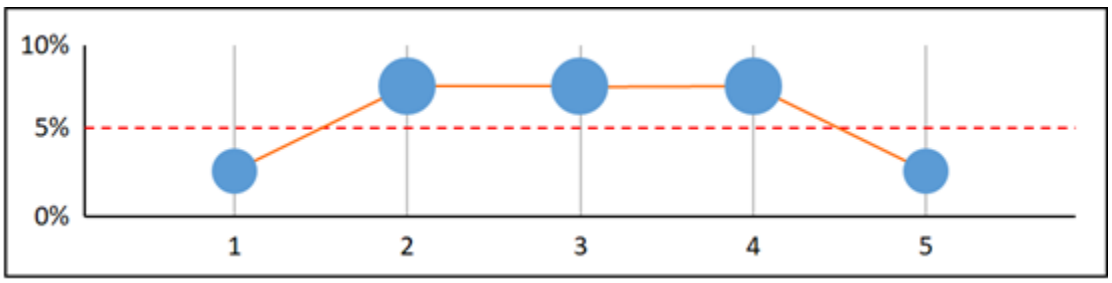
Beispiel für Alarm

Unter Berücksichtigung der zuvor beschriebenen Alarmbedingungen können Sie einen Alarm konfigurieren, der in einen `ALARM`-Zustand wechselt, wenn die CPU-Auslastung einer Instance einmal innerhalb von 5 Minuten mindestens 5 Prozent beträgt. Das folgende Beispiel zeigt die Einstellungen für diesen Alarm in der Lightsail-Konsole.



Wenn in diesem Beispiel die CPU-Auslastungsmetrik der Instance eine Auslastung von 5 Prozent oder mehr in nur einem Datenpunkt meldet, wechselt der Alarm aus dem Zustand `OK` in den Zustand `ALARM`. Jeder weitere gemeldete Datenpunkt mit einer Auslastung von mindestens 5 Prozent hält den Alarm im Zustand `ALARM`. Wenn die CPU-Auslastungsmetrik der Instance eine Auslastung von 4,9 Prozent oder weniger in nur einem Datenpunkt meldet, wechselt der Alarm aus dem Zustand `ALARM` in den Zustand `OK`.

Die folgende Grafik veranschaulicht diesen Alarm weiter. Die gepunktete rote Linie stellt den Schwellenwert für die CPU-Auslastung von 5 % dar. Die blauen Punkte stehen für metrische Datenpunkte. Der Alarm befindet sich für den ersten Datenpunkt im Zustand `OK`. Der zweite Datenpunkt ändert den Alarm in den Zustand `ALARM`, da der Datenpunkt größer als der Schwellenwert ist. Der dritte und vierte Datenpunkt behalten den Zustand `ALARM` bei, da die Datenpunkte weiterhin größer als der Schwellenwert sind. Der fünfte Datenpunkt ändert den Alarm in den Zustand `OK`, da der Datenpunkt kleiner als der Schwellenwert ist.



Konfigurieren der Behandlung fehlender Daten durch Alarme

In einigen Fällen werden einige Datenpunkte für eine Metrik mit einem Alarm nicht gemeldet. Dies kann beispielsweise passieren, wenn eine Verbindung unterbrochen wird oder ein Server ausfällt.

In Lightsail können Sie festlegen, wie fehlende Datenpunkte bei der Konfiguration eines Alarms behandelt werden sollen. Dadurch können Sie Ihren Alarm so konfigurieren, dass er in den ALARM-Zustand übergeht, wenn dies für die Art der überwachten Daten sinnvoll ist. Sie können Fehlalarme vermeiden, wenn fehlende Daten kein Problem darstellen.

Genauso wie sich jeder Alarm immer in einem von drei Status befindet, fällt jeder gemeldete Datenpunkt unter eine dieser drei Kategorien:

- Nicht überschreitend – Der Datenpunkt liegt innerhalb des Schwellenwerts.

  Beispiel: Wenn Sie den Vergleichsoperator greater than (größer als) gewählt haben, ist der Datenpunkt `Not breaching`, wenn er kleiner als der angegebene Schwellenwert ist. Wenn Sie den Vergleichsoperator less than (kleiner als) gewählt haben, ist der Datenpunkt `Not breaching`, wenn er größer als der angegebene Schwellenwert ist.
- Überschreitend – Der Datenpunkt ist außerhalb des Schwellenwerts.

  Beispiel: Wenn Sie den Vergleichsoperator greater than (größer als) gewählt haben, ist der Datenpunkt `Breaching`, wenn er größer als der angegebene Schwellenwert ist. Wenn Sie den Vergleichsoperator less than (kleiner als) gewählt haben, ist der Datenpunkt `Breaching`, wenn er kleiner als der angegebene Schwellenwert ist.
- Fehlend – Das Verhalten für fehlende Datenpunkten wird durch den `treat missing data`-Parameter angegeben.

Sie können für jeden Alarm angeben, wie Lightsail fehlende Datenpunkte behandeln soll:

- Nicht überschreitend – Fehlende Datenpunkte werden als „gültig“ und innerhalb der Schwelle liegend behandelt.
- Überschreitend – Fehlende Datenpunkte werden als „ungültig“ und außerhalb der Schwelle liegend behandelt.
- Ignorieren – Der aktuelle Alarmstatus wird beibehalten.
- Fehlend – Der Alarm berücksichtigt nicht fehlende Datenpunkte bei der Auswertung, ob ein Statuswechsel erfolgen soll. Dies ist das Standardverhalten für Alarme.

Die beste Wahl ist abhängig von der Art der Metrik. Bei einer Metrik, z. B. der CPU-Auslastung einer Instance, können Sie fehlende Datenpunkte als Verstoß behandeln. Dies liegt daran, dass die fehlenden Datenpunkte möglicherweise auf ein Problem hinweisen. Bei einer Metrik, die Datenpunkte nur bei Fehlern generiert, wie z. B. die HTTP 500-Serverfehleranzahl eines Load Balancers, sollten Sie fehlende Daten nicht als Verstoß behandeln.

Durch Auswahl der besten Option für Ihren Alarm verhindern Sie unnötige und irreführende Alarmzustandsänderungen. Zudem wird der Zustand Ihres Systems genauer angezeigt.

Wie der Alarmstatus bei fehlenden Daten ausgewertet wird

Unabhängig davon, welchen Wert Sie für die Behandlung fehlender Daten festlegen, wenn ein Alarm auswertet, ob der Status geändert werden soll, versucht Lightsail eine größere Anzahl von Datenpunkten abzurufen als durch Evaluation Period (Auswertungszeitraum) angegeben. Die genaue Anzahl der Datenpunkte, die abgerufen werden sollen, hängt von der Länge des Alarmzeitraums ab. Der Zeitrahmen der Datenpunkte, die sie abzurufen versucht, ist der Auswertungsbereich.

Nachdem Lightsail diese Datenpunkte abgerufen hat, geschieht Folgendes:

- Wenn keine Datenpunkte im Auswertungsbereich fehlen, wertet Lightsail den Alarm anhand der zuletzt erfassten Datenpunkte aus.
- Wenn einige Datenpunkte im Auswertungsbereich fehlen, aber die Anzahl der erfassten Datenpunkte gleich oder größer ist als die Evaluation Periods (Auswertungszeiträume) des Alarms, wertet Lightsail den Alarmstatus anhand der zuletzt erfolgreich erfassten Datenpunkte aus. In diesem Fall wird der von Ihnen eingestellte Wert für die Behandlung fehlender Daten nicht benötigt und dann ignoriert.
- Wenn einige Datenpunkte im Auswertungsbereich fehlen und die Anzahl der vorhandenen Datenpunkte, die erfasst wurden, niedriger ist als die Anzahl der Auswertungszeiträume des Alarms, füllt Lightsail die fehlenden Datenpunkte mit dem Ergebnis aus, das Sie für die Behandlung fehlender Daten angegeben haben, und wertet dann den Alarm aus. Allerdings werden alle realen Datenpunkte im Auswertungsbereich, unabhängig davon, wann sie erfasst wurden, in die Auswertung einbezogen. Lightsail verwendet fehlende Datenpunkte nur so selten wie möglich.

In all diesen Situationen entspricht die Anzahl der ausgewerteten Datenpunkte dem Wert von Evaluation Periods (Auswertungszeiträume). Wenn weniger als der Wert von Datapoints to Alarm (Datenpunkte zum Alarm) den Schwellenwert überschreiten, wird der Alarmstatus auf OK gesetzt. Andernfalls wird der Status auf ALARM gesetzt.

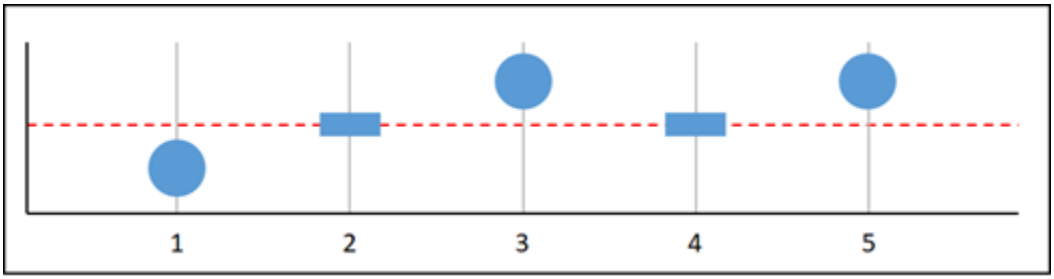
> **Note**
>
> Ein besonderer Fall dieses Verhaltens ist, dass Lightsail-Alarme den letzten Satz von Datenpunkten für einen bestimmten Zeitraum wiederholt neu auswerten können, nachdem die Metrik nicht mehr funktioniert hat. Diese Neuauswertung kann dazu führen, dass der Alarm den Status ändert und Aktionen erneut ausführt, wenn er den Status unmittelbar vor dem Stoppen des Messdatenstroms geändert hatte. Um dieses Verhalten zu verhindern, verwenden Sie kürzere Zeiträume.

Fehlende Daten in Grafikbeispielen

Die folgenden Diagramme in diesem Abschnitt veranschaulichen Beispiele für das Verhalten der Alarmauswertung. In den Diagrammen A, B, C, D und E sind die Zahlendatenpunkte, die zum Alarm überschritten werden müssen, und die Auswertungszeiträume jeweils 3. Die gepunktete rote Linie stellt den Schwellenwert dar, die blauen Punkte stellen gültige Datenpunkte dar und die Striche stellen fehlende Daten dar. Datenpunkte oberhalb der Linie für den gültigen Bereich stellen einen Verstoß dar, Datenpunkte darunter nicht. Falls einige der letzten drei Datenpunkte fehlen, versucht Lightsail, zusätzliche gültige Datenpunkte abzurufen.

> **Note**
>
> Wenn Datenpunkte kurz nach dem Erstellen eines Alarms fehlen und die Metrik an Lightsail gemeldet wurde, bevor Sie den Alarm erstellt haben, ruft Lightsail bei der Auswertung des Alarms die neuesten Datenpunkte von vor dem Erstellen des Alarms ab.

Diagramm A

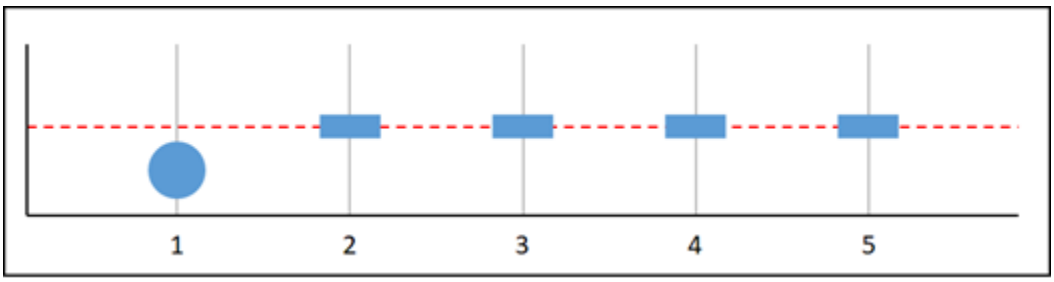


Im vorhergehenden Metrikdiagramm liegt Datenpunkt 1 im gültigen Bereich, Datenpunkt 2 fehlt, Datenpunkt 3 stellt einen Verstoß dar, Datenpunkt 4 fehlt und Datenpunkt 5 stellt ebenfalls einen

Verstoß dar. Da im Auswertungsbereich drei gültige Datenpunkte vorhanden sind, weist diese Metrik keine fehlenden Datenpunkte auf. Wenn Sie einen Alarm so konfiguriert haben, dass fehlende Datenpunkte folgendermaßen behandelt werden:

- Nicht überschreitend – Der Alarm würde in einem OK-Zustand sein.
- Überschreitend – Der Alarm würde in einem OK-Zustand sein.
- Ignorieren – Der Alarm würde in einem OK-Zustand sein.
- Fehlend – Der Alarm würde in einem OK-Zustand sein.

Diagramm B

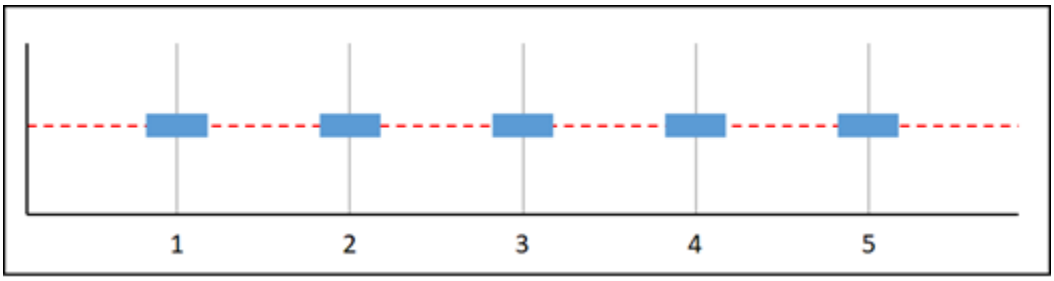


Im vorhergehenden Metrikdiagramm liegt der Datenpunkt 1 im gültigen Bereich und die Datenpunkte 2 bis 5 fehlen. Da im Auswertungsbereich nur ein Datenpunkt vorhanden ist, weist diese Metrik zwei fehlende Datenpunkte auf. Wenn Sie einen Alarm so konfiguriert haben, dass fehlende Datenpunkte folgendermaßen behandelt werden:

- Nicht überschreitend – Der Alarm würde in einem OK-Zustand sein.
- Überschreitend – Der Alarm würde in einem OK-Zustand sein.
- Ignorieren – Der Alarm würde in einem OK-Zustand sein.
- Fehlend – Der Alarm würde in einem OK-Zustand sein.

In diesem Szenario bleibt der Alarm im OK-Zustand, auch wenn fehlende Daten als Verstoß behandelt werden. Dies liegt daran, dass der eine vorhandene Datenpunkt keinen Verstoß darstellt und zusammen mit zwei fehlenden Datenpunkten ausgewertet wird, die als Verstoß behandelt werden. Wenn der Alarm das nächste Mal ausgewertet wird, wechselt er zu ALARM, wenn immer noch Daten fehlen. Dies liegt daran, dass ein Datenpunkt, der keinen Verstoß darstellt, nicht mehr zu den fünf zuletzt abgerufenen Datenpunkten gehört.

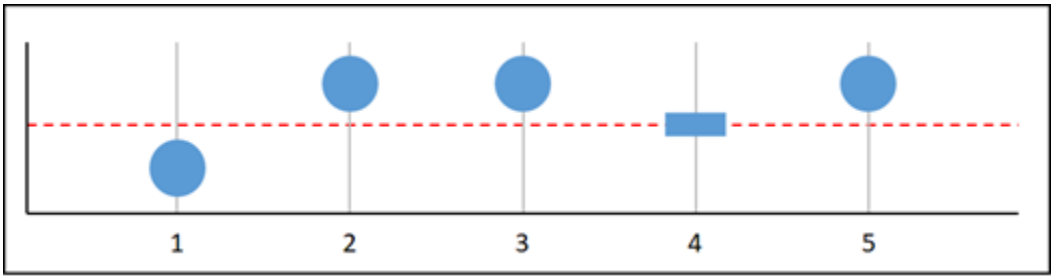
Diagramm C



Alle Datenpunkte fehlen in der vorhergehenden grafischen Metrik. Da alle Datenpunkte im Auswertungsbereich fehlen, weist diese Metrik drei fehlende Datenpunkte auf. Wenn Sie einen Alarm so konfiguriert haben, dass fehlende Datenpunkte folgendermaßen behandelt werden:

- Nicht überschreitend – Der Alarm würde in einem OK-Zustand sein.
- Überschreitend – Der Alarm würde in einem ALARM-Zustand sein.
- Ignorieren – Der Alarm würde den aktuellen Status beibehalten.
- Fehlend – Der Alarm würde im INSUFFICIENT_DATA-Status sein.

Diagramm D

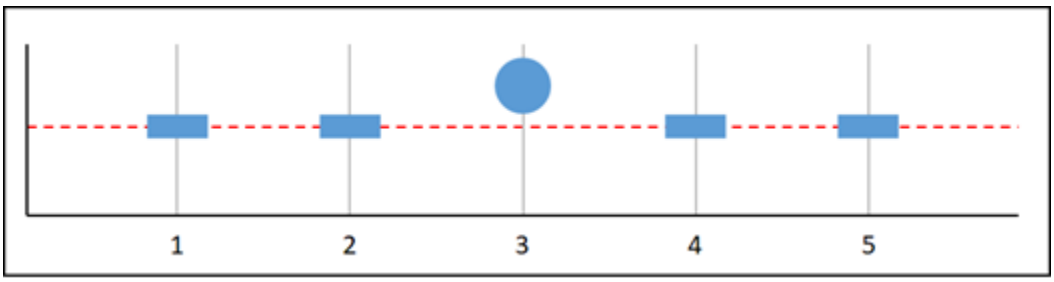


Im vorhergehenden Metrikdiagramm liegt Datenpunkt 1 im gültigen Bereich, Datenpunkt 2 stellt einen Verstoß dar, Datenpunkt 3 stellt einen Verstoß dar, Datenpunkt 4 fehlt und Datenpunkt 5 stellt einen Verstoß dar. Da im Auswertungsbereich vier gültige Datenpunkte vorhanden sind, weist diese Metrik keine fehlenden Datenpunkte auf. Wenn Sie einen Alarm so konfiguriert haben, dass fehlende Datenpunkte folgendermaßen behandelt werden:

- Nicht überschreitend – Der Alarm würde in einem ALARM-Zustand sein.
- Überschreitend – Der Alarm würde in einem ALARM-Zustand sein.
- Ignorieren – Der Alarm würde in einem ALARM-Zustand sein.
- Fehlend – Der Alarm würde in einem ALARM-Zustand sein.

In diesem Szenario wechselt der Alarm in allen Fällen in den ALARM-Zustand. Dies ist der Fall, da genügend reale Datenpunkte vorhanden sind, dass die Einstellung für die Behandlung fehlender Daten nicht erforderlich ist und dann ignoriert wird.

Diagramm E

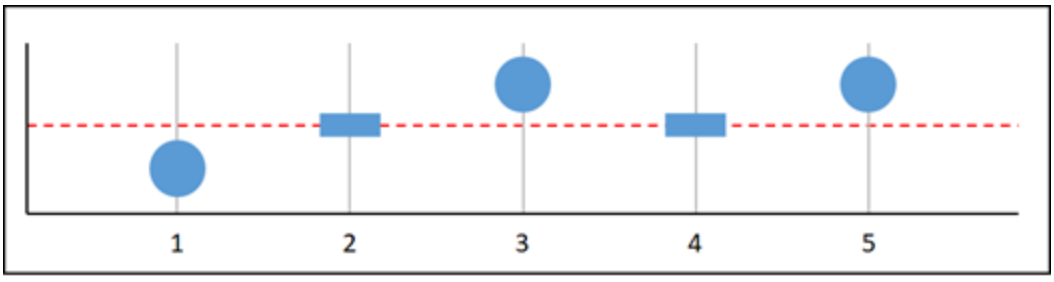


Im vorhergehenden Metrikdiagramm fehlen die Datenpunkte 1 und 2, der Datenpunkt 3 stellt einen Verstoß dar und die Datenpunkte 4 und 5 fehlen. Da im Auswertungsbereich nur ein Datenpunkt vorhanden ist, weist diese Metrik zwei fehlende Datenpunkte auf. Wenn Sie einen Alarm so konfiguriert haben, dass fehlende Datenpunkte folgendermaßen behandelt werden:

- Nicht überschreitend – Der Alarm würde in einem OK-Zustand sein.
- Überschreitend – Der Alarm würde in einem ALARM-Zustand sein.
- Ignorieren – Der Alarm würde den aktuellen Status beibehalten.
- Fehlend – Der Alarm würde in einem ALARM-Zustand sein.

In den Diagrammen F, G, H, I und J lautet Datenpunkte für Alarm 2, während der Wert für Auswertungszeiträume 3 ist. Dies ist ein 2-aus-3, M-aus-N-Alarm. 5 ist der Auswertungsbereich für den Alarm.

Diagramm F

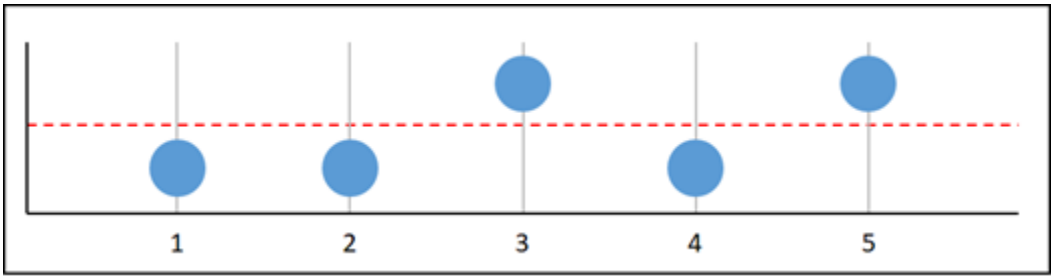


Im vorhergehenden Metrikdiagramm liegt Datenpunkt 1 im gültigen Bereich, Datenpunkt 2 fehlt, Datenpunkt 3 stellt einen Verstoß dar, Datenpunkt 4 fehlt und Datenpunkt 5 stellt einen Verstoß dar. Da im Auswertungsbereich drei Datenpunkte vorhanden sind, weist diese Metrik keine fehlenden

Datenpunkte auf. Wenn Sie einen Alarm so konfiguriert haben, dass fehlende Datenpunkte folgendermaßen behandelt werden:

- Nicht überschreitend – Der Alarm würde in einem ALARM-Zustand sein.
- Überschreitend – Der Alarm würde in einem ALARM-Zustand sein.
- Ignorieren – Der Alarm würde in einem ALARM-Zustand sein.
- Fehlend – Der Alarm würde in einem ALARM-Zustand sein.

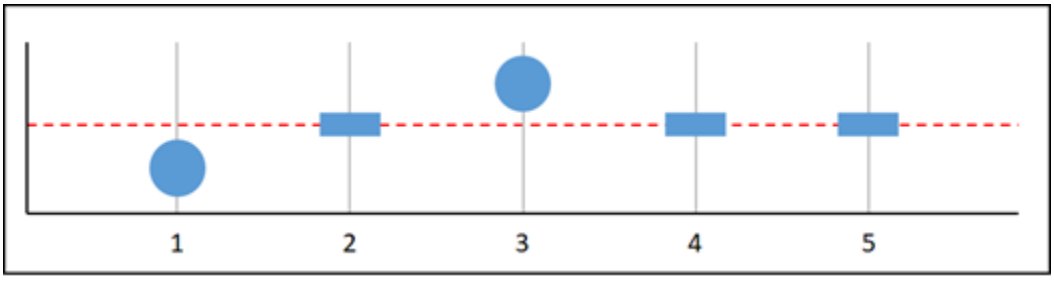
Diagramm G



Im vorhergehenden Metrikdiagramm liegen die Datenpunkte 1 und 2 im gültigen Bereich, Datenpunkt 3 stellt einen Verstoß dar, Datenpunkt 4 liegt im gültigen Bereich und Datenpunkt 5 stellt einen Verstoß dar. Da im Auswertungsbereich fünf Datenpunkte vorhanden sind, weist diese Metrik keine fehlenden Datenpunkte auf. Wenn Sie einen Alarm so konfiguriert haben, dass fehlende Datenpunkte folgendermaßen behandelt werden:

- Nicht überschreitend – Der Alarm würde in einem ALARM-Zustand sein.
- Überschreitend – Der Alarm würde in einem ALARM-Zustand sein.
- Ignorieren – Der Alarm würde in einem ALARM-Zustand sein.
- Fehlend – Der Alarm würde in einem ALARM-Zustand sein.

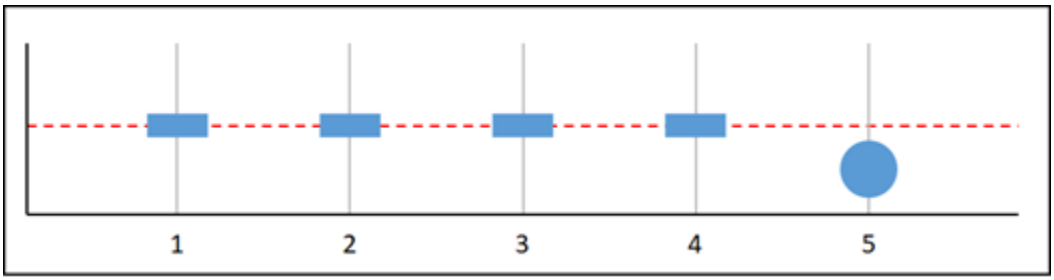
Diagramm H



Im vorhergehenden Metrikdiagramm liegt Datenpunkt 1 im gültigen Bereich, Datenpunkt 2 fehlt, Datenpunkt 3 stellt einen Verstoß dar und die Datenpunkte 4 und 5 fehlen. Da im Auswertungsbereich zwei Datenpunkte vorhanden sind, weist diese Metrik einen fehlenden Datenpunkt auf. Wenn Sie einen Alarm so konfiguriert haben, dass fehlende Datenpunkte folgendermaßen behandelt werden:

- Nicht überschreitend – Der Alarm würde in einem OK-Zustand sein.
- Überschreitend – Der Alarm würde in einem ALARM-Zustand sein.
- Ignorieren – Der Alarm würde in einem OK-Zustand sein.
- Fehlend – Der Alarm würde in einem OK-Zustand sein.

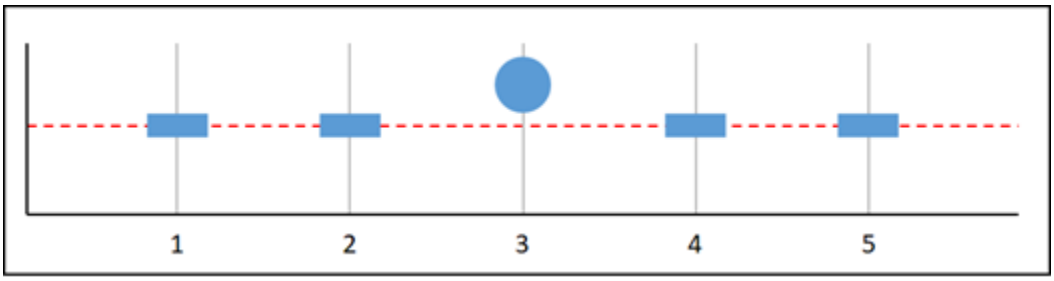
Diagramm I



Im vorhergehenden Metrikdiagramm fehlen die Datenpunkte 1 bis 4 und Datenpunkt 5 liegt im gültigen Bereich. Da im Auswertungsbereich ein Datenpunkt vorhanden ist, weist diese Metrik zwei fehlende Datenpunkte auf. Wenn Sie einen Alarm so konfiguriert haben, dass fehlende Datenpunkte folgendermaßen behandelt werden:

- Nicht überschreitend – Der Alarm würde in einem OK-Zustand sein.
- Überschreitend – Der Alarm würde in einem ALARM-Zustand sein.
- Ignorieren – Der Alarm würde in einem OK-Zustand sein.
- Fehlend – Der Alarm würde in einem OK-Zustand sein.

Diagramm J



Im vorhergehenden Metrikdiagramm fehlen die Datenpunkte 1 und 2, der Datenpunkt 3 stellt einen Verstoß dar und die Datenpunkte 4 und 5 fehlen. Da im Auswertungsbereich ein Datenpunkt vorhanden ist, weist diese Metrik zwei fehlende Datenpunkte auf. Wenn Sie einen Alarm so konfiguriert haben, dass fehlende Datenpunkte folgendermaßen behandelt werden:

- Nicht überschreitend – Der Alarm würde in einem OK-Zustand sein.
- Überschreitend – Der Alarm würde in einem ALARM-Zustand sein.
- Ignorieren – Der Alarm würde den aktuellen Status beibehalten.
- Fehlend – Der Alarm würde in einem ALARM-Zustand sein.

Weitere Informationen zu Alarmen

Im Folgenden finden Sie einige Artikel, mit denen Sie Alarme in Lightsail verwalten können:

- Instance-Metrikalarme erstellen
- Datenbank-Metrikalarme erstellen
- Load Balancer-Metrikalarm erstellen
- Verteilungs-Metrikalarmen erstellen
- Löschen oder Deaktivieren von Metrikalarmen

Erstellen von Lightsail-Instance-Metrikalarmen

Sie können einen Amazon Lightsail-Alarm erstellen, der eine einzelne Instance-Metrik überwacht. Ein Alarm kann so konfiguriert werden, dass Sie basierend auf dem Wert der Metrik relativ zu einem von Ihnen angegebenen Schwellenwert benachrichtigt werden. Benachrichtigungen können ein in der Lightsail-Konsole angezeigtes Banner, eine an Ihre E-Mail-Adresse gesendete E-Mail oder eine an Ihre Mobiltelefonnummer gesendete SMS-Nachricht sein. Weitere Informationen über Alarme finden Sie unter Alarme.

Inhalt

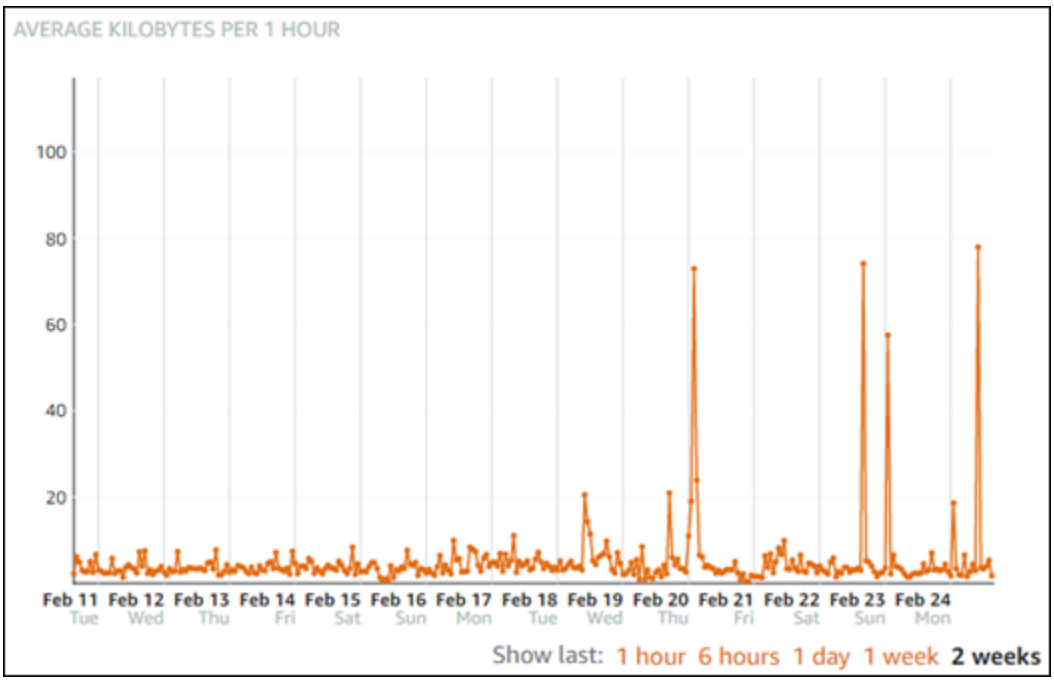
Instance-Alarmgrenzen

Die folgenden Limits gelten für Alarme:

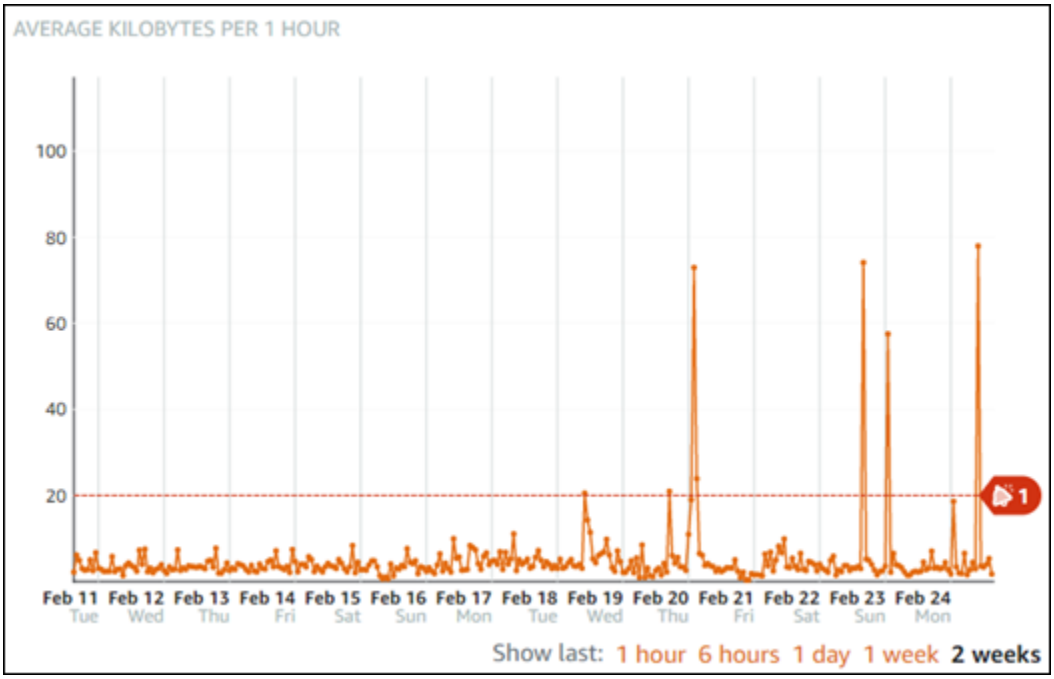
- Sie können zwei Alarme pro Metrik konfigurieren.
- Alarme werden in Intervallen von 5 Minuten ausgewertet. Jeder Datenpunkt für Alarme stellt einen Zeitraum von 5 Minuten aggregierter Metrikdaten dar.
- Sie können einen Alarm so konfigurieren, dass Sie nur dann benachrichtigt werden, wenn sich der Alarmzustand in `OK` ändert, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden.
- Sie können die `OK`-Alarmbenachrichtigung nur testen, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden.
- Sie können einen Alarm so konfigurieren, dass Sie nur dann benachrichtigt werden, wenn sich der Alarmstatus in `INSUFFICIENT_DATA` ändert, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden, und wenn Sie die Option Do not evaluate the missing data (Fehlende Daten nicht auswerten) für fehlende Datenpunkte wählen.
- Sie können Benachrichtigungen nur testen, wenn sich der Alarm im OK-Zustand befindet.

Bewährte Methoden zum Konfigurieren von Instance-Alarmen

Bevor Sie einen Metrikalarm für Ihre Instance konfigurieren, sollten Sie die historischen Daten der Metrik anzeigen. Ermitteln Sie das niedrige, mittlere und hohe Niveau der Metrik im Zeitraum der letzten beiden Wochen. Im folgenden Beispiel eines Metrikdiagramms für ausgehenden Netzwerkverkehr (`NetworkOut`) liegen das niedrige Niveau bei 0-10 KB pro Stunde, das mittlere Niveau zwischen 10-20 KB pro Stunde und das hohe Niveau zwischen 20-80 KB pro Stunde.



Wenn Sie den Alarmschwellenwert so konfigurieren, dass er im niedrigen Bereich (z. B. greater than or equal to (größer oder gleich) 5 KB pro Stunde) liegt, erhalten Sie häufigere und möglicherweise nicht erforderliche Alarmbenachrichtigungen. Wenn Sie den Alarmschwellenwert so konfigurieren, dass er im hohen Bereich (z. B. greater than or equal (größer oder gleich) 20 KB pro Stunde) liegt, erhalten Sie seltenere Alarmbenachrichtigungen, die allerdings genau untersucht werden müssen. Wenn Sie einen Alarm konfigurieren und aktivieren, wird im Diagramm wie im folgenden Beispiel eine Alarmlinie angezeigt, die den Schwellenwert darstellt. Die mit 1 beschriftete Alarmlinie stellt den Schwellenwert für Alarm 1 und die mit 2 beschriftete Alarmlinie den Schwellenwert für Alarm 2 dar.



Standardalarmeinstellungen

Die Standardalarmeinstellungen werden automatisch ausgefüllt, wenn Sie einen neuen Alarm in der Lightsail-Konsole hinzufügen. Dies ist die empfohlene Alarmkonfiguration für die ausgewählte Metrik. Sie sollten jedoch überprüfen, ob die standardmäßige Alarmkonfiguration für Ihre Ressource geeignet ist. Beispiel: Der standardmäßige Alarmschwellenwert für die Metrik des ausgehenden Netzwerkverkehrs (`NetworkOut`) der Instance ist innerhalb der letzten 10 Minuten 2 Mal less than or equal to (kleiner oder gleich) 0 Bytes. Wenn Sie jedoch über ein Ereignis mit hohem Datenverkehr benachrichtigt werden möchten, sollten Sie den Alarmschwellenwert so ändern, dass er zweimal innerhalb der letzten 10 Minuten größer oder gleich 50 KB ist, oder einen zweiten Alarm mit diesen Einstellungen hinzufügen, damit Sie benachrichtigt werden, wenn kein Datenverkehr vorhanden ist und wenn ein hoher Datenverkehr vorliegt. Der von Ihnen angegebene Schwellenwert sollte so angepasst werden, dass er dem oberen und unteren Grenzwert der Metrik entspricht, wie im Abschnitt Bewährte Methoden zum Konfigurieren von Instance-Alarmen dieses Handbuchs beschrieben.

Erstellen von Instance-Metrikalarmen über die Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um mithilfe der Lightsail-Konsole einen Instance-Metrikalarm zu erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Instances.

3. Wählen Sie den Namen der Instance, für die Sie Alarme erstellen möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Seite der Instance-Verwaltung aus.
5. Wählen Sie im Dropdown-Menü unter der Überschrift Metrics Graphs (Metrikdiagramme) die Metrik aus, für die Sie einen Alarm erstellen möchten. Weitere Informationen finden Sie unter Ressourcenmetriken.
6. Wählen Sie Alarm hinzufügen im Abschnitt Alarme der Seite.
7. Wählen Sie im Dropdown-Menü einen Vergleichsoperatorwert aus. Beispielwerte sind „Größer als oder gleich“, „Größer als“, „Kleiner als“ oder „Kleiner als oder gleich“.
8. Geben Sie einen Schwellenwert für den Alarm ein.
9. Geben Sie die Datenpunkte für den Alarm ein.
10. Wählen Sie die Bewertungszeiträume. Der Zeitraum kann in 5-Minuten-Schritten von 5 Minuten bis hin zu 24 Stunden angegeben werden.
11. Wählen Sie eine der folgenden Benachrichtigungsmethoden:

    - E-Mail: Sie werden per E-Mail benachrichtigt, wenn sich der Alarmzustand in ALARM ändert.
    - SMS-Textnachricht: Sie werden per SMS-Textnachricht benachrichtigt, wenn sich der Alarmzustand in ALARM ändert. SMS-Nachrichten werden nicht in allen AWS-Regionen unterstützt, in denen Sie Lightsail-Ressourcen erstellen können. SMS-Textnachrichten können nicht in alle Länder/Regionen gesendet werden. Weitere Informationen finden Sie unter Unterstützung von SMS-Textnachrichten.

    > **Note**
    >
    > Sie müssen eine E-Mail-Adresse oder Mobiltelefonnummer hinzufügen, wenn Sie sich für eine Benachrichtigung per E-Mail oder SMS entscheiden, aber noch keinen Benachrichtigungskontakt in der AWS-Region der Ressource konfiguriert haben. Weitere Informationen finden Sie unter Metrik-Benachrichtigungen.

12. (Optional) Wählen Sie Send me a notification when the alarm state change to OK (Benachrichtigung senden, wenn sich der Alarmzustand in OK ändert), um benachrichtigt zu werden, wenn der Alarmzustand zu OK wechselt. Diese Option ist nur verfügbar, wenn Sie per E-Mail oder SMS-Textnachricht benachrichtigt werden möchten.
13. (Optional) Wählen Sie Advanced settings (Erweiterte Einstellungen) und dann eine der folgenden Optionen:

- Legen Sie fest, wie der Alarm fehlende Daten behandeln soll. Folgende Optionen stehen zur Verfügung:
  - Angenommen, sie liegen nicht innerhalb des zulässigen Bereichs (Schwellenwert überschritten): Fehlende Datenpunkte werden als fehlerhaft behandelt und liegen außerhalb des gültigen Bereichs.
  - Angenommen, sie liegen innerhalb des gültigen Bereichs (Schwellenwert nicht überschritten): Fehlende Datenpunkte werden als ordnungsgemäß betrachtet und liegen innerhalb des gültigen Bereichs.
  - Den Wert des letzten gültigen Datenpunkts verwenden (Ignorieren und aktuellen Alarmzustand beibehalten) – Der aktuelle Alarmzustand wird beibehalten.
  - Nicht bewerten (Fehlende Daten als fehlend Daten behandeln): Bei der Bewertung, ob der Status geändert werden soll, werden fehlende Datenpunkte nicht berücksichtigt.
- Wählen Sie Send a notification if there is insufficient data (Benachrichtigung senden, wenn nicht genügend Daten vorhanden) sind, um benachrichtigt zu werden, wenn der Alarmzustand in INSUFFICIENT_DATA geändert wird. Diese Option ist nur verfügbar, wenn Sie per E-Mail oder SMS-Textnachricht benachrichtigt werden möchten.

14. Wählen Sie Create (Erstellen), um den Alarm hinzuzufügen.

    Um den Alarm später zu bearbeiten, wählen Sie das Ellipsensymbol (⋮) neben dem Alarm, den Sie bearbeiten möchten, und wählen Sie Alarm bearbeiten.

Testen von Instance-Metrikalarmen über die Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um einen Alarm über die Lightsail-Konsole zu testen. Sie können einen Alarm testen, um zu bestätigen, dass die konfigurierten Benachrichtigungsoptionen funktionieren, um beispielsweise sicherzustellen, dass Sie bei Auslösung des Alarms eine E-Mail oder eine SMS-Textnachricht erhalten.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Instances.
3. Wählen Sie den Namen der Instance, für die Sie einen Alarm testen möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Seite der Instance-Verwaltung aus.
5. Wählen Sie im Dropdown-Menü unter der Überschrift Metrics Graphs (Metrikdiagramme) die Metrik aus, für die Sie einen Alarm testen möchten.

6. Scrollen Sie nach unten zum Abschnitt Alarme und wählen Sie neben dem zu testenden Alarm das Ellipsensymbol (⋮) aus.
7. Wählen Sie eine der folgenden Optionen:

   - Alarmbenachrichtigung testen – Wählen Sie diese Option, um die Benachrichtigungen zu testen, wenn sich der Alarmstatus zu `ALARM` ändert.
   - OK-Benachrichtigung testen – Wählen Sie diese Option, um die Benachrichtigungen zu testen, wenn sich der Alarmstatus zu `OK` ändert.

   > **Note**
   >
   > Wenn eine dieser Optionen nicht verfügbar ist, haben Sie die Benachrichtigungsoptionen für den Alarm möglicherweise nicht konfiguriert, oder der Alarm befindet sich derzeit in einem `ALARM`-Zustand. Weitere Informationen finden Sie unter Instance-Alarmbeschränkungen.

   Der Alarm ändert sich je nach ausgewählter Testoption vorübergehend in den Zustand `OK` oder `ALARM`, und je nachdem, was Sie als Benachrichtigungsmethode für den Alarm konfiguriert haben, wird eine E-Mail und/oder SMS-Textnachricht gesendet. Ein Benachrichtigungsbanner wird nur dann in der Lightsail-Konsole angezeigt, wenn Sie die `ALARM`-Benachrichtigung testen möchten. Ein Benachrichtigungsbanner wird nicht angezeigt, wenn Sie die `OK`-Benachrichtigung testen möchten. Der Alarm kehrt oft nach einigen Sekunden in seinen tatsächlichen Zustand zurück.

Nächste Schritte

Es gibt einige zusätzliche Aufgaben, die Sie für Ihre Instance-Alarme ausführen können:

- Wenn Sie keine Benachrichtigungen mehr erhalten möchten, können Sie Ihre E-Mail und Ihre Mobiltelefonnummer aus Lightsail entfernen. Weitere Informationen finden Sie unter Löschen von Benachrichtigungskontakten. Sie können einen Alarm auch deaktivieren oder löschen, wenn Sie keine Benachrichtigungen für einen bestimmten Alarm mehr erhalten möchten. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen.

Löschen oder Deaktivieren von Lightsail-Metrikalarmen

Sie können einen Amazon Lightsail-Alarm löschen, wenn Sie nicht benachrichtigt werden möchten, sobald die vom Alarm überwachte Metrik einen Schwellenwert überschreitet. Sie können den Alarm auch deaktivieren, wenn Sie keine Benachrichtigungen mehr empfangen möchten. Weitere Informationen finden Sie unter -Alarme.

Inhalt

Metrikalarme mithilfe der Lightsail-Konsole löschen

Führen Sie die folgenden Schritte aus, um einen Metrikalarm über die Lightsail-Konsole zu löschen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Homepage die Registerkarte Instances, Datenbanken oder Netzwerk aus.
3. Wählen Sie den Namen der Ressource (Instance, Datenbank oder Load Balancer), für die Sie einen Alarm löschen möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Verwaltungsseite der Ressource.
5. Wählen Sie in der Dropdownliste unter der Überschrift Metrics Graphs (Metrikdiagramme) die Metrik aus, für die Sie einen Alarm löschen möchten.
6. Scrollen Sie nach unten zum Abschnitt Alarme und wählen Sie neben dem zu löschenden Alarm das Ellipsensymbol (⋮) aus.
7. Wählen Sie Delete (Löschen).
8. Wählen Sie bei der Eingabeaufforderung Delete (Löschen) aus, um das Löschen des Alarms zu bestätigen.

Deaktivieren und Aktivieren von Metrikalarmen über die Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um einen Metrikalarm über die Lightsail-Konsole zu deaktivieren.

1. Melden Sie sich an der Lightsail-Konsole an.

2. Wählen Sie auf der Lightsail-Homepage die Registerkarte Instances, Datenbanken oder Netzwerk aus.
3. Wählen Sie den Namen der Ressource (Instance, Datenbank oder Load Balancer), für die Sie einen Alarm deaktivieren möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Verwaltungsseite der Ressource.
5. Wählen Sie in der Dropdownliste unter der Überschrift Metrics Graphs (Metrikdiagramme) die Metrik aus, für die Sie einen Alarm deaktivieren möchten.
6. Scrollen Sie nach unten zum Abschnitt Alarms (Alarme), suchen Sie den Alarm, den Sie deaktivieren möchten, und betätigen Sie zum Deaktivieren den Umschalter. Genauso können Sie den Alarm mithilfe des Umschalters aktivieren, falls er deaktiviert ist.

Anzeigen von Lightsail-Bucket-Metriken

Nachdem Sie einen Bucket im Amazon Lightsail-Objektspeicherservice erstellt haben, können Sie die Metrikdiagramme auf der Registerkarte Metriken der Verwaltungsseite des Buckets anzeigen. Die Überwachung von Metriken ist ein wichtiger Teil, um die Zuverlässigkeit, Verfügbarkeit und Performance Ihrer Ressourcen aufrechtzuerhalten. Überwachen und sammeln Sie regelmäßig Metrikdaten von Ihrem Bucket, damit Sie bei Bedarf den Speicherplatz und das Netzwerkübertragungskontingent Ihres Buckets hoch- oder verkleinern können. Weitere Informationen zu Metriken erhalten Sie unter Ressourcenmetriken.

Bei der Überwachung Ihrer Ressourcen sollten Sie einen Bereich für die normale Ressourcenleistung in Ihrer Umgebung festlegen. Anschließend können Sie Alarme in der Lightsail-Konsole konfigurieren, damit Sie benachrichtigt werden, wenn die Leistung Ihrer Ressourcen außerhalb der angegebenen Schwellenwerte liegt. Weitere Informationen finden Sie unter Benachrichtigungen und Alarme.

Bucket-Metriken

Die folgenden Metriken sind für verfügbar:

- Bucket-Größe – Die Menge der in einem Bucket gespeicherten Daten. Zur Berechnung dieses Werts wird die Größe aller (aktuellen und nicht aktuellen) Objekte im Bucket summiert – einschließlich der Größe aller Teile für sämtliche unvollständige mehrteilige Uploads in den Bucket.
- Anzahl Objekte – Die Gesamtzahl der Objekte, die in einem Bucket gespeichert sind. Zur Berechnung dieses Werts werden alle aktuellen und nicht aktuellen Objekte im Bucket sowie die Gesamtanzahl der Teile sämtlicher unvollständiger mehrteiliger Uploads in den Bucket gezählt.

> **Note**
>
> Bucket-Metrikdaten werden nicht gemeldet, wenn Ihr Bucket leer ist.

Anzeigen von Bucket-Metriken in der Lightsail-Konsole

Befolgen Sie die folgende Prozedur, um Bucket-Metriken in der Lightsail-Konsole anzuzeigen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen der Instance aus, für die Sie Metriken anzeigen möchten.
4. Wählen Sie die Registerkarte Metriken auf der Seite der Bucket-Verwaltung aus.
5. Wählen Sie die Metrik aus, die Sie im Dropdown-Menü unter der Überschrift Metrics graphs (Metrikdiagramme) anzeigen möchten.

   Das Diagramm zeigt eine visuelle Darstellung der Datenpunkte für die gewählte Metrik an.

   ScreenshottBD

   Im Metrikdiagramm können Sie die folgenden Aktionen ausführen:

   - Sie können die Ansicht des Diagramms ändern, um Daten für 1 Stunde, 6 Stunden, 1 Tag, 1 Woche und 2 Wochen anzuzeigen.
   - Sie können den Cursor auf einem Datenpunkt anhalten, um detaillierte Informationen zu diesem Datenpunkt anzuzeigen.
   - Sie können einen Alarm für die ausgewählte Metrik hinzufügen, damit Sie benachrichtigt werden, wenn die Metrik einen von Ihnen angegebenen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Alarme und Erstellen von Bucket-Metrikalarmen.

Verwalten von Buckets und Objekten

Dies sind die allgemeinen Schritte zum Verwalten Ihres Lightsail-Objektspeicher-Buckets:

1. Weitere Informationen über Buckets und Objekte im Amazon Lightsail-Objektspeicherservice. Weitere Informationen zu Buckets finden Sie unter Objektspeicher in Amazon Lightsail.

2. Erfahren Sie mehr über die Namen, die Sie Ihren Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Namensregeln für Buckets in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherservice, indem Sie einen Bucket erstellen. Weitere Informationen finden Sie unter Buckets erstellen in Amazon Lightsail.
4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Lightsail-Objektspeicher und Bucket-Berechtigungen in Amazon Lightsail verstehen.

   Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

   - Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail
   - Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail
   - Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
   - Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
   - Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail
   - Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail
5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.

   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherservice
   - Zugriffsprotokollierungsformat für Buckets im Amazon Lightsail-Objektspeicher-Service
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicher-Service
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail, um Anforderungen zu identifizieren
6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gewährt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets in Amazon Lightsail.

7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unterGrundlegendes zu Objektschlüsselnamen inAmazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Hochladen einer Datei in einen Bucket in Amazon Lightsail
   - Hochladen von Dateien in Buckets in Amazon Lightsail mit mehrteiligem Upload
   - Anzeigen von Objekten in einem Bucket in Amazon Lightsail
   - Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
   - Objekte von einem Bucket in Amazon Lightsail herunterladen
   - Filtern von Objekten in einem Bucket in Amazon Lightsail
   - Markieren von Objekten in einem Bucket in Amazon Lightsail
   - Löschen von Objekten in einem Bucket in Amazon Lightsail
9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.
10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.
11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.
12. Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen in Amazon Lightsail.
13. Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Tarifs Ihres Buckets in Amazon Lightsail.
14. Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.
   - Tutorial: Verbinden einer WordPress-Instance mit einem Amazon Lightsail-Bucket
   - Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Lightsail-Netzwerkverteilung für die Bereitstellung von Inhalten
15. Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

Themen

Erstellen von Lightsail-Bucket-Metrikalarmen

Sie können einen Amazon Lightsail-Alarm erstellen, der eine einzelne Bucket-Metrik überwacht. Ein Alarm kann so konfiguriert werden, dass Sie basierend auf dem Wert der Metrik relativ zu einem von Ihnen angegebenen Schwellenwert benachrichtigt werden. Benachrichtigungen können ein in der Lightsail-Konsole angezeigtes Banner, eine an Ihre E-Mail-Adresse gesendete E-Mail oder eine an Ihre Mobiltelefonnummer gesendete SMS-Nachricht sein. Weitere Informationen über Alarme finden Sie unter Alarme.

Inhalt

Limits für Bucket-Alarme

Die folgenden Limits gelten für Alarme:

- Sie können zwei Alarme pro Metrik konfigurieren.
- Alarme werden in Intervallen von 5 Minuten ausgewertet. Jeder Datenpunkt für Alarme stellt einen Zeitraum von 5 Minuten aggregierter Metrikdaten dar.
- Sie können einen Alarm so konfigurieren, dass Sie nur dann benachrichtigt werden, wenn sich der Alarmzustand in `OK` ändert, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden.
- Sie können die `OK`-Alarmbenachrichtigung nur testen, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden.
- Sie können einen Alarm so konfigurieren, dass Sie nur dann benachrichtigt werden, wenn sich der Alarmstatus in `INSUFFICIENT_DATA` ändert, wenn Sie den Alarm so konfigurieren, dass Sie

per E-Mail und/oder SMS-Textnachricht benachrichtigt werden, und wenn Sie die Option Do not evaluate the missing data (Fehlende Daten nicht auswerten) für fehlende Datenpunkte wählen.

- Sie können Benachrichtigungen nur testen, wenn sich der Alarm im OK-Zustand befindet.

Bewährte Methoden zum Konfigurieren von Bucket-Alarmen

Bevor Sie einen Metrikalarm für Ihren Bucket konfigurieren, sollten Sie festlegen, worüber Sie benachrichtigt werden möchten. Wenn Sie beispielsweise den Messwert Bucket-Größe beachten wollen, möchten Sie möglicherweise benachrichtigt werden, wenn Ihr Bucket fast voll ist. Wenn Ihr aktueller Bucket-Plan 5 GB Speicherplatz umfasst, möchten Sie möglicherweise einen Alarm für die Metrik Bucket-Größe konfigurieren, wenn diese 4,5 GB erreicht. Dann sollten Sie rechtzeitig benachrichtigt werden, um den Tarif Ihres Buckets zu erweitern.

Standardalarmeinstellungen

Die Standardalarmeinstellungen werden automatisch vorausgefüllt, wenn Sie einen neuen Alarm in der Lightsail-Konsole hinzufügen. Dies ist die empfohlene Alarmkonfiguration für die ausgewählte Metrik. Sie sollten jedoch überprüfen, ob die standardmäßige Alarmkonfiguration für Ihre Ressource geeignet ist. Der Standardalarmschwellenwert für die Metrik Bucketgröße in Bytes ist beispielsweise größer oder gleich 75 GB. Dieser Anforderungsschwellenwert ist jedoch möglicherweise zu hoch für Ihren Bucket, wenn er nur für 5 GB Speicherplatz konfiguriert ist. Möglicherweise möchten Sie den Alarmschwellenwert so ändern, dass er gleich oder größer als 4,5 GB ist.

Erstellen von Bucket-Metrikalarmen mit der Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um mithilfe der Lightsail-Konsole einen Bucket-Metrikalarm zu erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen des Buckets aus, für den Sie Alarme erstellen möchten.
4. Wählen Sie die Registerkarte Metriken auf der Seite der Bucket-Verwaltung aus.
5. Wählen Sie im Dropdown-Menü unter der Überschrift Metrics Graphs (Metrikdiagramme) die Metrik aus, für die Sie einen Alarm erstellen möchten. Weitere Informationen finden Sie unter Ressourcenmetriken.
6. Wählen Sie Alarm hinzufügen im Abschnitt Alarme der Seite.

7. Wählen Sie im Dropdown-Menü einen Vergleichsoperatorwert aus. Beispielwerte sind „Größer als oder gleich“, „Größer als“, „Kleiner als“ oder „Kleiner als oder gleich“.
8. Geben Sie einen Schwellenwert für den Alarm ein.
9. Geben Sie die Datenpunkte für den Alarm ein.
10. Wählen Sie die Bewertungszeiträume. Der Zeitraum kann in 5-Minuten-Schritten von 5 Minuten bis hin zu 24 Stunden angegeben werden.
11. Wählen Sie eine der folgenden Benachrichtigungsmethoden:

    - E-Mail: Sie werden per E-Mail benachrichtigt, wenn sich der Alarmzustand in ALARM ändert.
    - SMS-Textnachricht: Sie werden per SMS-Textnachricht benachrichtigt, wenn sich der Alarmzustand in ALARM ändert. SMS-Nachrichten werden nicht in allen AWS-Regionen unterstützt und SMS-Textnachrichten können nicht in alle Länder/Regionen gesendet werden. Weitere Informationen finden Sie unter Unterstützung von SMS-Textnachrichten.

    > **Note**
    >
    > Sie müssen eine E-Mail-Adresse oder Mobiltelefonnummer hinzufügen, wenn Sie sich für eine Benachrichtigung per E-Mail oder SMS entscheiden, aber noch keinen Benachrichtigungskontakt in der AWS-Region der Ressource konfiguriert haben. Weitere Informationen finden Sie unter Benachrichtigungen.

12. (Optional) Wählen Sie Send me a notification when the alarm state change to OK (Benachrichtigung senden, wenn sich der Alarmzustand in OK ändert), um benachrichtigt zu werden, wenn der Alarmzustand zu OK wechselt. Diese Option ist nur verfügbar, wenn Sie per E-Mail oder SMS-Textnachricht benachrichtigt werden möchten.
13. (Optional) Wählen Sie Advanced settings (Erweiterte Einstellungen) und dann eine der folgenden Optionen:

    - Legen Sie fest, wie der Alarm fehlende Daten behandeln soll. Folgende Optionen stehen zur Verfügung:
        - Angenommen, sie liegen nicht innerhalb des zulässigen Bereichs (Schwellenwert überschritten): Fehlende Datenpunkte werden als fehlerhaft behandelt und liegen außerhalb des gültigen Bereichs.

- Angenommen, sie liegen innerhalb des gültigen Bereichs (Schwellenwert nicht überschritten): Fehlende Datenpunkte werden als ordnungsgemäß betrachtet und liegen innerhalb des gültigen Bereichs.
- Den Wert des letzten gültigen Datenpunkts verwenden (Ignorieren und aktuellen Alarmzustand beibehalten) – Der aktuelle Alarmzustand wird beibehalten.
- Nicht bewerten (Fehlende Daten als fehlend Daten behandeln): Bei der Bewertung, ob der Status geändert werden soll, werden fehlende Datenpunkte nicht berücksichtigt.

- Wählen Sie Send a notification if there is insufficient data (Benachrichtigung senden, wenn nicht genügend Daten vorhanden) sind, um benachrichtigt zu werden, wenn der Alarmzustand in INSUFFICIENT_DATA geändert wird. Diese Option ist nur verfügbar, wenn Sie per E-Mail oder SMS-Textnachricht benachrichtigt werden möchten.

14. Wählen Sie Create (Erstellen), um den Alarm hinzuzufügen.

    Um den Alarm später zu bearbeiten, wählen Sie das Ellipsensymbol (⋮) neben dem Alarm, den Sie bearbeiten möchten, und wählen Sie Alarm bearbeiten.

Testen von Bucket-Metrikalarmen mit der Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um einen Alarm über die Lightsail-Konsole zu testen. Sie können einen Alarm testen, um zu bestätigen, dass die konfigurierten Benachrichtigungsoptionen funktionieren, um beispielsweise sicherzustellen, dass Sie bei Auslösung des Alarms eine E-Mail oder eine SMS-Textnachricht erhalten.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Storage (Speicher) aus.
3. Wählen Sie den Namen des Buckets aus, für den Sie einen Alarm testen möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Seite der Bucket-Verwaltung aus.
5. Wählen Sie im Dropdown-Menü unter der Überschrift Metrics Graphs (Metrikdiagramme) die Metrik aus, für die Sie einen Alarm testen möchten.
6. Scrollen Sie nach unten zum Abschnitt Alarme und wählen Sie neben dem zu testenden Alarm das Ellipsensymbol (⋮) aus.
7. Wählen Sie eine der folgenden Optionen:

    - Alarmbenachrichtigung testen – Wählen Sie diese Option, um die Benachrichtigungen zu testen, wenn sich der Alarmstatus zu `ALARM` ändert.

- OK-Benachrichtigung testen – Wählen Sie diese Option, um die Benachrichtigungen zu testen, wenn sich der Alarmstatus zu `OK` ändert.

> **Note**
>
> Wenn eine dieser Optionen nicht verfügbar ist, haben Sie die Benachrichtigungsoptionen für den Alarm möglicherweise nicht konfiguriert, oder der Alarm befindet sich derzeit in einem `ALARM`-Zustand. Weitere Informationen finden Sie unter Bucket-Alarm-Beschränkungen.

Der Alarm ändert sich je nach ausgewählter Testoption vorübergehend in den Zustand `OK` oder `ALARM`, und je nachdem, was Sie als Benachrichtigungsmethode für den Alarm konfiguriert haben, wird eine E-Mail und/oder SMS-Textnachricht gesendet. Ein Benachrichtigungsbanner wird nur dann in der Lightsail-Konsole angezeigt, wenn Sie die `ALARM`-Benachrichtigung testen möchten. Ein Benachrichtigungsbanner wird nicht angezeigt, wenn Sie die `OK`-Benachrichtigung testen möchten. Der Alarm kehrt oft nach einigen Sekunden in seinen tatsächlichen Zustand zurück.

Nächste Schritte nach dem Erstellen von Bucket-Alarmen

Es gibt einige zusätzliche Aufgaben, die Sie für Ihre Bucket-Alarme ausführen können:

- Wenn Sie keine Benachrichtigungen mehr erhalten möchten, können Sie Ihre E-Mail und Ihre Mobiltelefonnummer aus Lightsail entfernen. Weitere Informationen finden Sie unter Löschen von Benachrichtigungskontakten. Sie können einen Alarm auch deaktivieren oder löschen, wenn Sie keine Benachrichtigungen für einen bestimmten Alarm mehr erhalten möchten. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen.

Lightsail-Container-Service-Metriken anzeigen

Nachdem Sie einen Bucket im Amazon Lightsail-Container-Service erstellt haben, können Sie die Metrikdiagramme auf der Registerkarte „Metriken“ der Verwaltungsseite des Buckets anzeigen. Die Überwachung von Metriken ist ein wichtiger Teil, um die Zuverlässigkeit, Verfügbarkeit und Performance Ihrer Ressourcen aufrechtzuerhalten. Überwachen und sammeln Sie regelmäßig

Metrikdaten von Ihren Ressourcen, damit Sie bei Auftreten eines Mehrpunkt-Fehlers diesen leichter debuggen können. Weitere Informationen zu Metriken finden Sie unter Metriken in Amazon Lightsail.

Bei der Überwachung Ihrer Ressourcen sollten Sie einen Bereich für die normale Ressourcenleistung in Ihrer Umgebung festlegen.

> **Note**
>
> Alarme und Benachrichtigungen werden derzeit für Container-Servicemetriken nicht unterstützt.

Container-Service-Metriken

Die folgenden Containermetriken sind verfügbar:

- CPU-Nutzung – Der durchschnittliche Prozentsatz der Recheneinheiten, die gegenwärtig auf allen Knoten Ihres Container-Servicess verwendet werden. Diese Metrik gibt die erforderliche Rechenleistung an, um Container-Services auszuführen.
- Speicherauslastung – Der durchschnittliche Prozentsatz des Speichers, der derzeit auf allen Knoten des Container-Servicess verwendet wird. Diese Metrik identifiziert den Speicher, der zum Ausführen von Containern in Ihrem Container-Service erforderlich ist.

> **Note**
>
> Wenn Sie eine neue Bereitstellung erstellen, verschwinden die vorhandenen Auslastungsmetriken Ihres Container-Servicess, und es werden nur Metriken für die neue aktuelle Bereitstellung angezeigt.

Container-Service-Metriken in der Lightsail-Konsole anzeigen

Führen Sie die folgenden Verfahren vollständig aus, um Container-Service-Metriken in der Lightsail-Konsole anzuzeigen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Container.

3. Wählen Sie den Namen der Containers aus, für den Sie Metriken anzeigen möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Verwaltungsseite Ihres Container-Servicess.
5. Wählen Sie die Metrik aus, die Sie im Dropdown-Menü unter der Überschrift Metrics graphs (Metrikdiagramme) anzeigen möchten.

   Das Diagramm zeigt eine visuelle Darstellung der Datenpunkte für die gewählte Metrik an.
6. Im Metrikdiagramm können Sie die folgenden Aktionen ausführen:

   - Sie können die Ansicht des Diagramms ändern, um Daten für 1 Stunde, 6 Stunden, 1 Tag, 1 Woche und 2 Wochen anzuzeigen.
   - Sie können den Cursor auf einem Datenpunkt anhalten, um detaillierte Informationen zu diesem Datenpunkt anzuzeigen.

   > **Note**
   >
   > Alarme und Benachrichtigungen werden derzeit für Container-Servicemetriken nicht unterstützt.

Lightsail-Datenbankmetriken anzeigen

Nachdem Sie eine Datenbank in Amazon Lightsail gestartet haben, können Sie die Metrikdiagramme auf der Registerkarte Metrics (Metriken) der Verwaltungsseite der Datenbank anzeigen. Die Überwachung von Metriken ist ein wichtiger Teil, um die Zuverlässigkeit, Verfügbarkeit und Performance Ihrer Ressourcen aufrechtzuerhalten. Überwachen und sammeln Sie regelmäßig Metrikdaten von Ihren Ressourcen, damit Sie bei Auftreten eines Mehrpunkt-Fehlers diesen leichter debuggen können. Weitere Informationen zu Metriken finden Sie unter Metriken.

Bei der Überwachung Ihrer Ressourcen sollten Sie einen Bereich für die normale Ressourcenleistung in Ihrer Umgebung festlegen. Nachdem Sie einen Grundwert erstellt haben, können Sie in der Lightsail-Konsole Alarme konfigurieren, damit Sie benachrichtigt werden, wenn Ihre Ressourcen außerhalb der festgelegten Schwellenwerte arbeiten. Weitere Informationen finden Sie unter Benachrichtigungen und Alarme.

Inhalt

Datenbankmetriken

Die folgenden Datenbankmetriken sind verfügbar:

- CPU-Auslastung (**`CPUUtilization`**) – Prozentsatz der CPU-Auslastung, die gegenwärtig in der Datenbank verwendet wird.
- Datenbankverbindungen (**`DatabaseConnections`**) – Anzahl der genutzten Datenbankverbindungen.
- Tiefe der Datenträgerwarteschlange (**`DiskQueueDepth`**) – Anzahl der offenstehenden E/A (Lese-/Schreibanforderungen), die auf den Datenträger zugreifen möchten.
- Freier Speicherplatz (**`FreeStorageSpace`**) – Die Menge an verfügbarem Speicherplatz.
- Netzwerkempfangsdurchsatz (**`NetworkReceiveThroughput`**) – Der eingehende (Receive) Netzwerkverkehr auf der Datenbank, einschließlich Kundendatenbankverkehr und AWS-Datenverkehr, der für Überwachung und Replikation verwendet wird.
- Netzwerkausgangsdurchsatz (**`NetworkTransmitThroughput`**) – Der ausgehende (Transmit) Netzwerkverkehr auf der Datenbank, einschließlich Kundendatenbankverkehr und AWS-Datenverkehr, der für Überwachung und Replikation verwendet wird.

Anzeigen von Datenbankmetriken in der Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um Datenbankmetriken in der Lightsail-Konsole anzuzeigen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Databases (Datenbanken) aus.
3. Wählen Sie den Namen der Datenbank, für die Sie die Metriken anzeigen möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Seite „Datenbankverwaltung“.
5. Wählen Sie die Metrik aus, die Sie im Dropdown-Menü unter der Überschrift Metrics graphs (Metrikdiagramme) anzeigen möchten.

   Das Diagramm zeigt eine visuelle Darstellung der Datenpunkte für die gewählte Metrik an.
6. Im Metrikdiagramm können Sie die folgenden Aktionen ausführen:

- Sie können die Ansicht des Diagramms ändern, um Daten für 1 Stunde, 6 Stunden, 1 Tag, 1 Woche und 2 Wochen anzuzeigen.
- Sie können den Cursor auf einem Datenpunkt anhalten, um detaillierte Informationen zu diesem Datenpunkt anzuzeigen.
- Sie können einen Alarm für die ausgewählte Metrik hinzufügen, damit Sie benachrichtigt werden, wenn die Metrik einen von Ihnen angegebenen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Alarme und Erstellen von Datenbank-Metrikalarmen.

Nächste Schritte nach dem Anzeigen Ihrer Datenbankmetriken

Sie können einige zusätzliche Aufgaben für Ihre Datenbankmetriken ausführen:

- Sie können einen Alarm für die ausgewählte Metrik hinzufügen, damit Sie benachrichtigt werden, wenn die Metrik einen von Ihnen angegebenen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Alarme und Erstellen von Datenbank-Metrikalarmen.
- Wenn ein Alarm ausgelöst wird, wird ein Benachrichtigungsbanner in der Lightsail-Konsole angezeigt. Um per E-Mail und SMS benachrichtigt zu werden, müssen Sie in jeder AWS-Region, in der Sie Ihre Ressourcen überwachen möchten, Ihre E-Mail-Adresse und Mobiltelefonnummer als Benachrichtigungskontakt angeben. Weitere Informationen finden Sie unter Hinzufügen von Benachrichtigungskontakten.
- Wenn Sie keine Benachrichtigungen mehr erhalten möchten, können Sie Ihre E-Mail und Ihre Mobiltelefonnummer aus Lightsail entfernen. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen. Sie können einen Alarm auch deaktivieren oder löschen, wenn Sie keine Benachrichtigungen für einen bestimmten Alarm mehr erhalten möchten. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen.

Themen

- Alarme für Lightsail-Datenbankmetriken erstellen

Alarme für Lightsail-Datenbankmetriken erstellen

Sie können einen Amazon Lightsail-Alarm erstellen, der eine einzelne Datenbankmetrik überwacht. Ein Alarm kann so konfiguriert werden, dass Sie basierend auf dem Wert der Metrik relativ zu einem von Ihnen angegebenen Schwellenwert benachrichtigt werden. Benachrichtigungen können ein in der

Lightsail-Konsole angezeigtes Banner, eine an Ihre E-Mail-Adresse gesendete E-Mail oder eine an Ihre Mobiltelefonnummer gesendete SMS-Nachricht sein. Weitere Informationen über Alarme finden Sie unter Alarme.

Inhalt

Datenbankalarmgrenzen

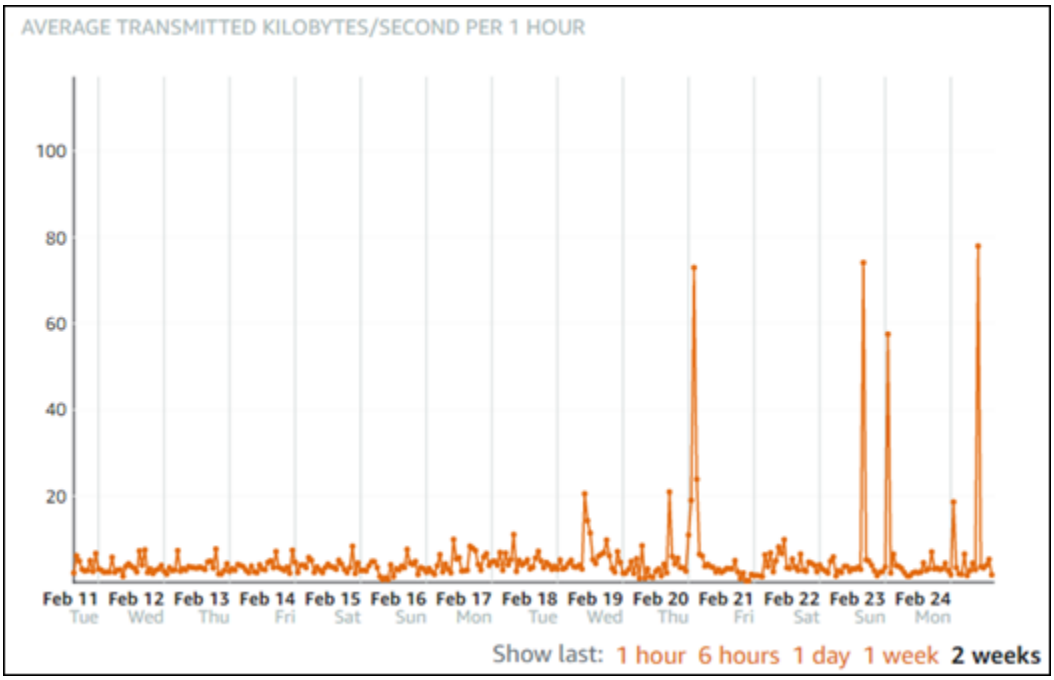
Die folgenden Limits gelten für Alarme:

- Sie können zwei Alarme pro Metrik konfigurieren.
- Alarme werden in Intervallen von 5 Minuten ausgewertet. Jeder Datenpunkt für Alarme stellt einen Zeitraum von 5 Minuten aggregierter Metrikdaten dar.
- Sie können einen Alarm so konfigurieren, dass Sie nur dann benachrichtigt werden, wenn sich der Alarmzustand in `OK` ändert, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden.
- Sie können die `OK`-Alarmbenachrichtigung nur testen, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden.
- Sie können einen Alarm so konfigurieren, dass Sie nur dann benachrichtigt werden, wenn sich der Alarmstatus in `INSUFFICIENT_DATA` ändert, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden, und wenn Sie die Option Do not evaluate the missing data (Fehlende Daten nicht auswerten) für fehlende Datenpunkte wählen.
- Sie können Benachrichtigungen nur testen, wenn sich der Alarm im OK-Zustand befindet.

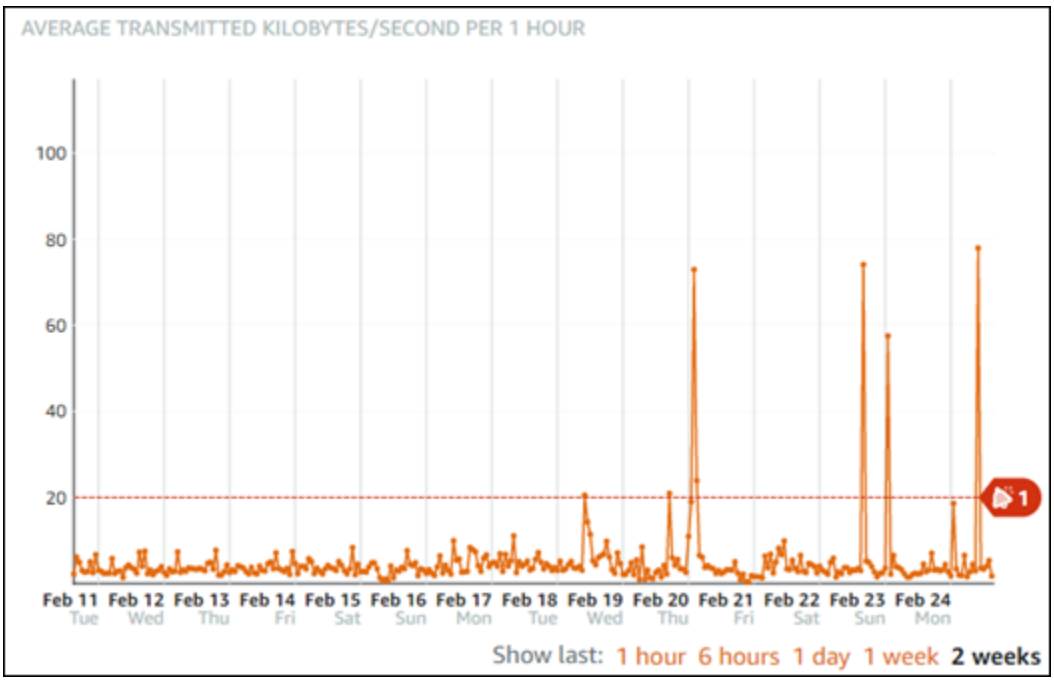
Bewährte Methoden zum Konfigurieren von Datenbankalarmen

Bevor Sie einen Metrikalarm für Ihre Datenbank konfigurieren, sollten Sie die historischen Daten der Metrik anzeigen. Ermitteln Sie das niedrige, mittlere und hohe Niveau der Metrik im Zeitraum

der letzten beiden Wochen. Im folgenden Metrikdiagramm für den Netzwerkübertragungsdurchsatz (`NetworkTransmitThroughput`) liegen das niedrige Niveau bei 0-10 KB/Sekunde pro Stunde, das mittlere Niveau bei 10-20 KB/Sekunde pro Stunde und das hohe Niveau bei 20-80 KB/Sekunde pro Stunde.



Wenn Sie den Alarmschwellenwert so konfigurieren, dass er im niedrigen Bereich (z. B. greater than or equal to (größer oder gleich) 5 KB/Sekunde pro Stunde) liegt, erhalten Sie häufigere und möglicherweise nicht erforderliche Alarmbenachrichtigungen. Wenn Sie den Alarmschwellenwert so konfigurieren, dass er im hohen Bereich (z. B. greater than or equal (größer oder gleich) 20 KB pro Stunde) liegt, erhalten Sie seltenere Alarmbenachrichtigungen, die allerdings genau untersucht werden müssen. Wenn Sie einen Alarm konfigurieren und aktivieren, wird im Diagramm wie im folgenden Beispiel eine Alarmlinie angezeigt, die den Schwellenwert darstellt. Die mit 1 beschriftete Alarmlinie stellt den Schwellenwert für Alarm 1 und die mit 2 beschriftete Alarmlinie den Schwellenwert für Alarm 2 dar.



Standardalarmeinstellungen

Die Standardalarmeinstellungen werden automatisch ausgefüllt, wenn Sie einen neuen Alarm in der Lightsail-Konsole hinzufügen. Dies ist die empfohlene Alarmkonfiguration für die ausgewählte Metrik. Sie sollten jedoch überprüfen, ob die standardmäßige Alarmkonfiguration für Ihre Ressource geeignet ist. Beispielsweise beträgt der standardmäßige Alarmschwellenwert der Metrik für freien Speicherplatz (`FreeStorageSpace`) 1 Mal innerhalb der vorherigen 5 Minuten less than (weniger als) 5 Byte. Dieser Schwellenwert für freien Speicherplatz ist jedoch möglicherweise zu niedrig für Ihre Datenbank. Sie können den Alarmschwellenwert so ändern, dass er 1 Mal innerhalb der vorherigen 5 Minuten less than (weniger als) 4 GB beträgt.

Erstellen von Datenbank-Metrikalarmen mit der Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um mithilfe der Lightsail-Konsole einen Datenbank-Metrikalarm zu erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Databases (Datenbanken) aus.
3. Wählen Sie den Namen der Datenbank, für die Sie Alarme erstellen möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Seite „Datenbankverwaltung“.

5. Wählen Sie im Dropdown-Menü unter der Überschrift Metrics Graphs (Metrikdiagramme) die Metrik aus, für die Sie einen Alarm erstellen möchten. Weitere Informationen finden Sie unter Ressourcenmetriken.
6. Wählen Sie Alarm hinzufügen im Abschnitt Alarme der Seite.
7. Wählen Sie im Dropdown-Menü einen Vergleichsoperatorwert aus. Beispielwerte sind „Größer als oder gleich“, „Größer als“, „Kleiner als“ oder „Kleiner als oder gleich“.
8. Geben Sie einen Schwellenwert für den Alarm ein.
9. Geben Sie die Datenpunkte für den Alarm ein.
10. Wählen Sie die Bewertungszeiträume. Der Zeitraum kann in 5-Minuten-Schritten von 5 Minuten bis hin zu 24 Stunden angegeben werden.
11. Wählen Sie eine der folgenden Benachrichtigungsmethoden:

    - E-Mail: Sie werden per E-Mail benachrichtigt, wenn sich der Alarmzustand in ALARM ändert.
    - SMS-Textnachricht: Sie werden per SMS-Textnachricht benachrichtigt, wenn sich der Alarmzustand in ALARM ändert. SMS-Nachrichten werden nicht in allen AWS-Regionen unterstützt, in denen Sie Lightsail-Ressourcen erstellen können. SMS-Textnachrichten können nicht in alle Länder/Regionen gesendet werden. Weitere Informationen finden Sie unter Unterstützung von SMS-Textnachrichten.

    > **Note**
    >
    > Sie müssen eine E-Mail-Adresse oder Mobiltelefonnummer hinzufügen, wenn Sie sich für eine Benachrichtigung per E-Mail oder SMS entscheiden, aber noch keinen Benachrichtigungskontakt in der AWS-Region der Ressource konfiguriert haben. Weitere Informationen finden Sie unter Benachrichtigungen.

12. (Optional) Wählen Sie Send me a notification when the alarm state change to OK (Benachrichtigung senden, wenn sich der Alarmzustand in OK ändert), um benachrichtigt zu werden, wenn der Alarmzustand zu OK wechselt. Diese Option ist nur verfügbar, wenn Sie per E-Mail oder SMS-Textnachricht benachrichtigt werden möchten.
13. (Optional) Wählen Sie Advanced settings (Erweiterte Einstellungen) und dann eine der folgenden Optionen:

    - Legen Sie fest, wie der Alarm fehlende Daten behandeln soll. Folgende Optionen stehen zur Verfügung:

- Angenommen, sie liegen nicht innerhalb des zulässigen Bereichs (Schwellenwert überschritten): Fehlende Datenpunkte werden als fehlerhaft behandelt und liegen außerhalb des gültigen Bereichs.
- Angenommen, sie liegen innerhalb des gültigen Bereichs (Schwellenwert nicht überschritten): Fehlende Datenpunkte werden als ordnungsgemäß betrachtet und liegen innerhalb des gültigen Bereichs.
- Den Wert des letzten gültigen Datenpunkts verwenden (Ignorieren und aktuellen Alarmzustand beibehalten) – Der aktuelle Alarmzustand wird beibehalten.
- Nicht bewerten (Fehlende Daten als fehlend Daten behandeln): Bei der Bewertung, ob der Status geändert werden soll, werden fehlende Datenpunkte nicht berücksichtigt.

- Wählen Sie Send a notification if there is insufficient data (Benachrichtigung senden, wenn nicht genügend Daten vorhanden) sind, um benachrichtigt zu werden, wenn der Alarmzustand in INSUFFICIENT_DATA geändert wird. Diese Option ist nur verfügbar, wenn Sie per E-Mail oder SMS-Textnachricht benachrichtigt werden möchten.

14. Wählen Sie Create (Erstellen), um den Alarm hinzuzufügen.

    Um den Alarm später zu bearbeiten, wählen Sie das Ellipsensymbol (⋮) neben dem Alarm, den Sie bearbeiten möchten, und wählen Sie Alarm bearbeiten.

Testen von Datenbank-Metrikalarmen mit der Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um einen Alarm über die Lightsail-Konsole zu testen. Sie können einen Alarm testen, um zu bestätigen, dass die konfigurierten Benachrichtigungsoptionen funktionieren, um beispielsweise sicherzustellen, dass Sie bei Auslösung des Alarms eine E-Mail oder eine SMS-Textnachricht erhalten.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Databases (Datenbanken) aus.
3. Wählen Sie den Namen der Datenbank, für die Sie einen Alarm testen möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Seite „Datenbankverwaltung“.
5. Wählen Sie im Dropdown-Menü unter der Überschrift Metrics Graphs (Metrikdiagramme) die Metrik aus, für die Sie einen Alarm testen möchten.
6. Scrollen Sie nach unten zum Abschnitt Alarme und wählen Sie neben dem zu testenden Alarm das Ellipsensymbol (⋮) aus.
7. Wählen Sie eine der folgenden Optionen:

- Alarmbenachrichtigung testen – Wählen Sie diese Option, um die Benachrichtigungen zu testen, wenn sich der Alarmstatus zu ALARM ändert.
- OK-Benachrichtigung testen – Wählen Sie diese Option, um die Benachrichtigungen zu testen, wenn sich der Alarmstatus zu OK ändert.

> **Note**
>
> Wenn eine dieser Optionen nicht verfügbar ist, haben Sie die Benachrichtigungsoptionen für den Alarm möglicherweise nicht konfiguriert, oder der Alarm befindet sich derzeit in einem ALARM-Zustand. Weitere Informationen finden Sie unter Datenbankalarmgrenzen.

Der Alarm ändert sich je nach ausgewählter Testoption vorübergehend in den Zustand OK oder ALARM, und je nachdem, was Sie als Benachrichtigungsmethode für den Alarm konfiguriert haben, wird eine E-Mail und/oder SMS-Textnachricht gesendet. Ein Benachrichtigungsbanner wird nur dann in der Lightsail-Konsole angezeigt, wenn Sie die ALARM-Benachrichtigung testen möchten. Ein Benachrichtigungsbanner wird nicht angezeigt, wenn Sie die OK-Benachrichtigung testen möchten. Der Alarm kehrt oft nach einigen Sekunden in seinen tatsächlichen Zustand zurück.

Nächste Schritte nach dem Erstellen von Datenbankalarmen

Sie können einige zusätzliche Aufgaben für Ihre Datenbankalarme ausführen:

- Wenn Sie keine Benachrichtigungen mehr erhalten möchten, können Sie Ihre E-Mail und Ihre Mobiltelefonnummer aus Lightsail entfernen. Weitere Informationen finden Sie unter Löschen von Benachrichtigungskontakten. Sie können einen Alarm auch deaktivieren oder löschen, wenn Sie keine Benachrichtigungen für einen bestimmten Alarm mehr erhalten möchten. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen.

Anzeigen von Lightsail-Verteilungsmetriken

Nachdem Sie eine Verteilung in Amazon Lightsail erstellt haben, können Sie die Metrikdiagramme auf der Registerkarte Metriken der Verteilungsverwaltung einsehen. Die Überwachung von Metriken ist ein wichtiger Teil, um die Zuverlässigkeit, Verfügbarkeit und Performance Ihrer Ressourcen

aufrechtzuerhalten. Überwachen und sammeln Sie regelmäßig Metrikdaten von Ihren Ressourcen, damit Sie bei Auftreten eines Mehrpunkt-Fehlers diesen leichter debuggen können. Weitere Informationen zu Metriken finden Sie unter Metriken.

Bei der Überwachung Ihrer Ressourcen sollten Sie einen Bereich für die normale Ressourcenleistung in Ihrer Umgebung festlegen. Anschließend können Sie Alarme in der Lightsail-Konsole konfigurieren, damit Sie benachrichtigt werden, wenn die Leistung Ihrer Ressourcen außerhalb der angegebenen Schwellenwerte liegt. Weitere Informationen finden Sie unter Benachrichtigungen und Alarme.

Inhalt

Verteilungsmetriken

Folgende Verteilungsmetriken sind verfügbar:

- Anforderungen – Die Gesamtzahl der von Ihrer Verteilung empfangenen Viewer-Anforderungen für alle HTTP-Methoden sowie für HTTP- und HTTPS-Anforderungen.
- Hochgeladene Bytes – Die Anzahl der Bytes, die von Ihrer Verteilung mithilfe von POST- und PUT-Anforderungen an Ihren Ursprung hochgeladen wurden.
- Heruntergeladene Bytes – Die Anzahl der von Viewern für GET-, HEAD- und OPTIONS-Anforderungen heruntergeladenen Bytes.
- Fehlerrate gesamt – Der Prozentsatz aller Viewer-Anforderungen, für die der HTTP-Statuscode der Antwort 4xx oder 5xx lautet.
- HTTP-4xx-Fehlerrate – Der Prozentsatz aller Viewer-Anforderungen, für die der HTTP-Statuscode der Antwort 4xx lautet. In diesen Fällen hat der Client oder Client-Viewer möglicherweise einen Fehler gemacht. Beispiel: 404 (nicht gefunden) bedeutet, dass der Client ein Objekt angefordert hat, das nicht gefunden wurde.
- HTTP-5xx-Fehlerrate – Der Prozentsatz aller Viewer-Anforderungen, für die der HTTP-Statuscode der Antwort 5xx lautet. In diesen Fällen hat der Ursprungsserver die Anforderung nicht erfüllt. Beispiel: 503 (Service nicht verfügbar) bedeutet, dass der Ursprungsserver zurzeit nicht verfügbar ist.

Anzeigen von Verteilungsmetriken in der Lightsail-Konsole

Befolgen Sie die folgende Prozedur, um Bucket-Metriken in der Lightsail-Konsole anzuzeigen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen der Datenbank, für die Sie die Metriken anzeigen möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Seite der Verteilungsverwaltung aus.
5. Wählen Sie die Metrik aus, die Sie im Dropdown-Menü unter der Überschrift Metrics graphs (Metrikdiagramme) anzeigen möchten.

   Das Diagramm zeigt eine visuelle Darstellung der Datenpunkte für die gewählte Metrik an.
6. Im Metrikdiagramm können Sie die folgenden Aktionen ausführen:

   - Sie können die Ansicht des Diagramms ändern, um Daten für 1 Stunde, 6 Stunden, 1 Tag, 1 Woche und 2 Wochen anzuzeigen.
   - Sie können den Cursor auf einem Datenpunkt anhalten, um detaillierte Informationen zu diesem Datenpunkt anzuzeigen.
   - Sie können einen Alarm für die ausgewählte Metrik hinzufügen, damit Sie benachrichtigt werden, wenn die Metrik einen von Ihnen angegebenen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Alarme und Erstellen von Instance-Metrikalarmen.

Nächste Schritte nach dem Anzeigen Ihrer Instance-Metriken

Es gibt einige zusätzliche Aufgaben, die Sie für Ihre Instance-Metriken ausführen können:

- Sie können einen Alarm für die ausgewählte Metrik hinzufügen, damit Sie benachrichtigt werden, wenn die Metrik einen von Ihnen angegebenen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Alarme und Erstellen von Verteilungs-Metrikalarmen.
- Wenn ein Alarm ausgelöst wird, wird ein Benachrichtigungsbanner in der Lightsail-Konsole angezeigt. Um per E-Mail und SMS benachrichtigt zu werden, müssen Sie in jeder AWS-Region, in der Sie Ihre Ressourcen überwachen möchten, Ihre E-Mail-Adresse und Mobiltelefonnummer als Benachrichtigungskontakt angeben. Weitere Informationen finden Sie unter Hinzufügen von Benachrichtigungskontakten.
- Wenn Sie keine Benachrichtigungen mehr erhalten möchten, können Sie Ihre E-Mail und Ihre Mobiltelefonnummer aus Lightsail entfernen. Weitere Informationen finden Sie unter Löschen

oder Deaktivieren von Metrikalarmen. Sie können einen Alarm auch deaktivieren oder löschen, wenn Sie keine Benachrichtigungen für einen bestimmten Alarm mehr erhalten möchten. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen.

Themen

Erstellen von Lightsail-Verteilungs-Metrikalarmen

Sie können einen Amazon Lightsail-Alarm erstellen, der eine einzelne Verteilung-Metrik überwacht. Ein Alarm kann so konfiguriert werden, dass Sie basierend auf dem Wert der Metrik relativ zu einem von Ihnen angegebenen Schwellenwert benachrichtigt werden. Benachrichtigungen können ein in der Lightsail-Konsole angezeigtes Banner, eine an Ihre E-Mail-Adresse gesendete E-Mail oder eine an Ihre Mobiltelefonnummer gesendete SMS-Nachricht sein. Weitere Informationen über Alarme finden Sie unter Alarme.

Inhalt

Verteilung-Alarm-Beschränkungen

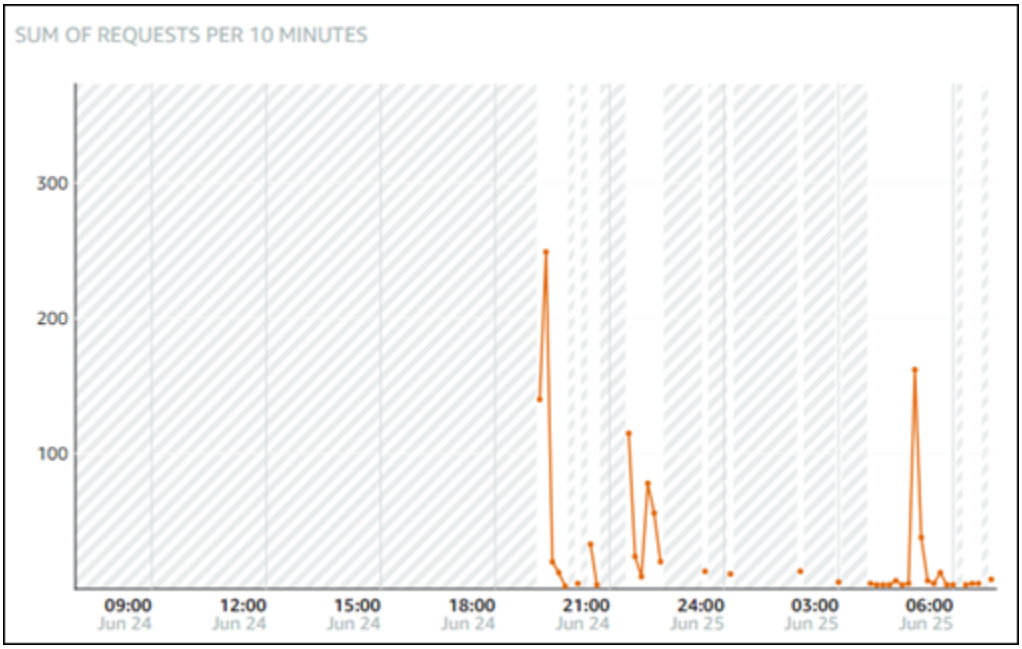
Die folgenden Limits gelten für Alarme:

- Sie können zwei Alarme pro Metrik konfigurieren.
- Alarme werden in Intervallen von 5 Minuten ausgewertet. Jeder Datenpunkt für Alarme stellt einen Zeitraum von 5 Minuten aggregierter Metrikdaten dar.
- Sie können einen Alarm so konfigurieren, dass Sie nur dann benachrichtigt werden, wenn sich der Alarmzustand in OK ändert, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden.

- Sie können die OK-Alarmbenachrichtigung nur testen, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden.
- Sie können einen Alarm so konfigurieren, dass Sie nur dann benachrichtigt werden, wenn sich der Alarmstatus in `INSUFFICIENT_DATA` ändert, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden, und wenn Sie die Option Do not evaluate the missing data (Fehlende Daten nicht auswerten) für fehlende Datenpunkte wählen.
- Sie können Benachrichtigungen nur testen, wenn sich der Alarm im OK-Zustand befindet.

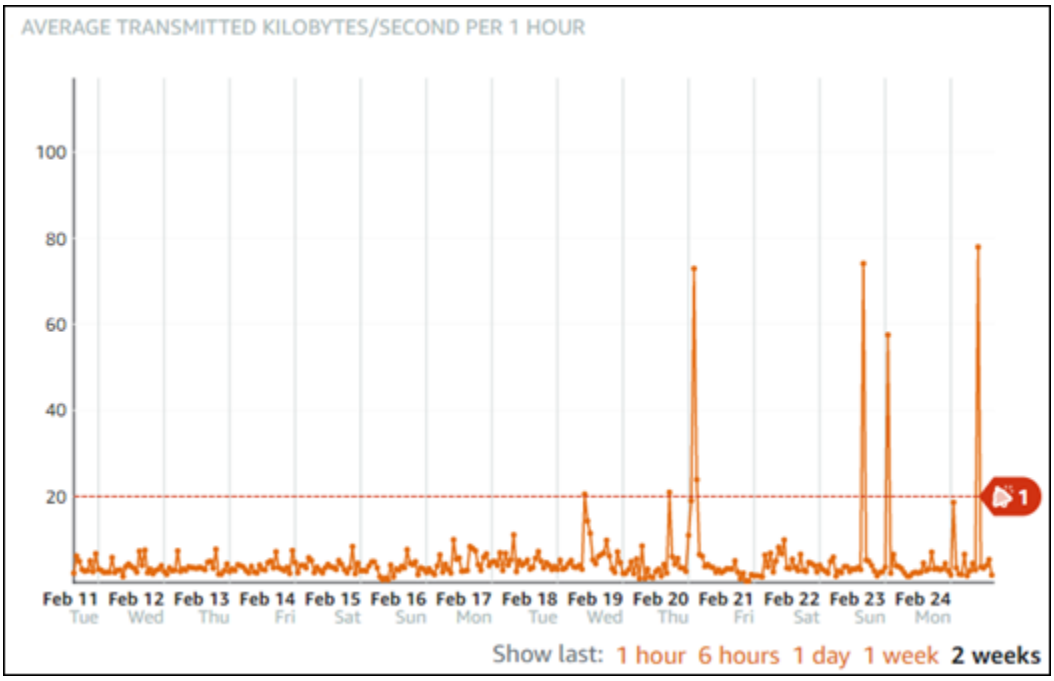
Bewährte Methoden zum Konfigurieren von Verteilung-Alarmen

Bevor Sie einen Metrikalarm für Ihre Verteilung konfigurieren, sollten Sie die historischen Daten der Metrik anzeigen. Ermitteln Sie das niedrige, mittlere und hohe Niveau der Metrik im Zeitraum der letzten beiden Wochen. Im folgenden Beispiel für ein Anforderung--Metrik-Diagramm sind die unteren Ebenen 0–10 Anforderungen, die mittleren Ebenen zwischen 10–50 Anforderungen und die oberen Ebenen zwischen 50–250 Anforderungen.



Wenn Sie den Alarm-Schwellenwert so konfigurieren, dass er größer oder gleich irgendwo im unteren Bereich liegt (z. B. 5 Anforderungen), erhalten Sie häufigere und möglicherweise unnötige Alarm-Benachrichtigungen. Wenn Sie den Alarm-Schwellenwert so konfigurieren, dass er größer oder gleich irgendwo im oberen Bereich liegt (z. B. 150 Anforderungen), erhalten Sie weniger häufig Alarmbenachrichtigungen, es könnte jedoch wichtiger sein, diese zu untersuchen. Wenn Sie einen Alarm konfigurieren und aktivieren, wird im Diagramm wie im folgenden Beispiel eine Alarmlinie

angezeigt, die den Schwellenwert darstellt. Die mit 1 beschriftete Alarmlinie stellt den Schwellenwert für Alarm 1 und die mit 2 beschriftete Alarmlinie den Schwellenwert für Alarm 2 dar.



Standardalarmeinstellungen

Die Standardalarmeinstellungen werden automatisch ausgefüllt, wenn Sie einen neuen Alarm in der Lightsail-Konsole hinzufügen. Dies ist die empfohlene Alarmkonfiguration für die ausgewählte Metrik. Sie sollten jedoch überprüfen, ob die standardmäßige Alarmkonfiguration für Ihre Ressource geeignet ist. Der Standard-Alarmschwellenwert für die Anfragen-Metrik ist z. B. größer als 3 Mal 45 Anfragen innerhalb der letzten 15 Minuten. Dieser Anforderungsschwellenwert ist jedoch möglicherweise für Ihre Verteilung zu niedrig. Möglicherweise möchten Sie den Alarmschwellenwert so ändern, dass er innerhalb der letzten 15 Minuten dreimal bei mehr als 150 Anforderungen liegt.

Verwenden Sie die Lightsail-Konsole zum Erstellen von Verteilungs-Metrikalarmen

Führen Sie die folgenden Schritte aus, um einen Verteilung-Metrikalarm mithilfe der Lightsail-Konsole zu erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie Namen der Verteilung aus, für die Sie Alarme erstellen möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Seite der Verteilungsverwaltung aus.

5. Wählen Sie im Dropdown-Menü unter der Überschrift Metrics Graphs (Metrikdiagramme) die Metrik aus, für die Sie einen Alarm erstellen möchten. Weitere Informationen finden Sie unter Ressourcenmetriken.
6. Wählen Sie Alarm hinzufügen im Abschnitt Alarme der Seite.
7. Wählen Sie im Dropdown-Menü einen Vergleichsoperatorwert aus. Beispielwerte sind „Größer als oder gleich“, „Größer als“, „Kleiner als“ oder „Kleiner als oder gleich“.
8. Geben Sie einen Schwellenwert für den Alarm ein.
9. Geben Sie die Datenpunkte für den Alarm ein.
10. Wählen Sie die Bewertungszeiträume. Der Zeitraum kann in 5-Minuten-Schritten von 5 Minuten bis hin zu 24 Stunden angegeben werden.
11. Wählen Sie eine der folgenden Benachrichtigungsmethoden:

    - E-Mail: Sie werden per E-Mail benachrichtigt, wenn sich der Alarmzustand in ALARM ändert.
    - SMS-Textnachricht: Sie werden per SMS-Textnachricht benachrichtigt, wenn sich der Alarmzustand in ALARM ändert. SMS-Nachrichten werden nicht in allen AWS-Regionen unterstützt, in denen Sie Lightsail-Ressourcen erstellen können. SMS-Textnachrichten können nicht in alle Länder/Regionen gesendet werden. Weitere Informationen finden Sie unter Unterstützung von SMS-Textnachrichten.

    > **Note**
    >
    > Sie müssen eine E-Mail-Adresse oder Mobiltelefonnummer hinzufügen, wenn Sie sich für eine Benachrichtigung per E-Mail oder SMS entscheiden, aber noch keinen Benachrichtigungskontakt in der AWS-Region der Ressource konfiguriert haben. Weitere Informationen finden Sie unter Benachrichtigungen.

12. (Optional) Wählen Sie Send me a notification when the alarm state change to OK (Benachrichtigung senden, wenn sich der Alarmzustand in OK ändert), um benachrichtigt zu werden, wenn der Alarmzustand zu OK wechselt. Diese Option ist nur verfügbar, wenn Sie per E-Mail oder SMS-Textnachricht benachrichtigt werden möchten.
13. (Optional) Wählen Sie Advanced settings (Erweiterte Einstellungen) und dann eine der folgenden Optionen:

    - Legen Sie fest, wie der Alarm fehlende Daten behandeln soll. Folgende Optionen stehen zur Verfügung:

- Angenommen, sie liegen nicht innerhalb des zulässigen Bereichs (Schwellenwert überschritten): Fehlende Datenpunkte werden als fehlerhaft behandelt und liegen außerhalb des gültigen Bereichs.
- Angenommen, sie liegen innerhalb des gültigen Bereichs (Schwellenwert nicht überschritten): Fehlende Datenpunkte werden als ordnungsgemäß betrachtet und liegen innerhalb des gültigen Bereichs.
- Den Wert des letzten gültigen Datenpunkts verwenden (Ignorieren und aktuellen Alarmzustand beibehalten): Der aktuelle Alarmzustand wird beibehalten.
- Nicht bewerten (Fehlende Daten als fehlend Daten behandeln): Bei der Bewertung, ob der Status geändert werden soll, werden fehlende Datenpunkte nicht berücksichtigt.

- Wählen Sie Send a notification if there is insufficient data (Benachrichtigung senden, wenn nicht genügend Daten vorhanden) sind, um benachrichtigt zu werden, wenn der Alarmzustand in INSUFFICIENT_DATA geändert wird. Diese Option ist nur verfügbar, wenn Sie per E-Mail oder SMS-Textnachricht benachrichtigt werden möchten.

14. Wählen Sie Create (Erstellen), um den Alarm hinzuzufügen.

    Um den Alarm später zu bearbeiten, wählen Sie das Ellipsensymbol (⋮) neben dem Alarm, den Sie bearbeiten möchten, und wählen Sie Alarm bearbeiten.

Testen von Verteilungs-Metrikalarmen

Führen Sie die folgenden Schritte aus, um einen Alarm über die Lightsail-Konsole zu testen. Sie können einen Alarm testen, um zu bestätigen, dass die konfigurierten Benachrichtigungsoptionen funktionieren, um beispielsweise sicherzustellen, dass Sie bei Auslösung des Alarms eine E-Mail oder eine SMS-Textnachricht erhalten.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen der Verteilung aus, für die Sie einen Alarm testen möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Seite der Verteilungsverwaltung aus.
5. Wählen Sie im Dropdown-Menü unter der Überschrift Metrics Graphs (Metrikdiagramme) die Metrik aus, für die Sie einen Alarm testen möchten.
6. Scrollen Sie nach unten zum Abschnitt Alarme und wählen Sie neben dem zu testenden Alarm das Ellipsensymbol (⋮) aus.
7. Wählen Sie eine der folgenden Optionen:

- Alarmbenachrichtigung testen – Wählen Sie diese Option, um die Benachrichtigungen zu testen, wenn sich der Alarmstatus zu ALARM ändert.
- OK-Benachrichtigung testen – Wählen Sie diese Option, um die Benachrichtigungen zu testen, wenn sich der Alarmstatus zu OK ändert.

> **Note**
>
> Wenn eine dieser Optionen nicht verfügbar ist, haben Sie die Benachrichtigungsoptionen für den Alarm möglicherweise nicht konfiguriert, oder der Alarm befindet sich derzeit in einem ALARM-Zustand. Weitere Informationen finden Sie unter Verteilung-Alarm-Beschränkungen.

Der Alarm ändert sich je nach ausgewählter Testoption vorübergehend in den Zustand OK oder ALARM, und je nachdem, was Sie als Benachrichtigungsmethode für den Alarm konfiguriert haben, wird eine E-Mail und/oder SMS-Textnachricht gesendet. Ein Benachrichtigungsbanner wird nur dann in der Lightsail-Konsole angezeigt, wenn Sie die ALARM-Benachrichtigung testen möchten. Ein Benachrichtigungsbanner wird nicht angezeigt, wenn Sie die OK-Benachrichtigung testen möchten. Der Alarm kehrt oft nach einigen Sekunden in seinen tatsächlichen Zustand zurück.

Nächste Schritte nach dem Erstellen von Verteilung-Alarmen

Es gibt einige zusätzliche Aufgaben, die Sie für Ihre Verteilung-Alarme ausführen können:

- Wenn Sie keine Benachrichtigungen mehr erhalten möchten, können Sie Ihre E-Mail und Ihre Mobiltelefonnummer aus Lightsail entfernen. Weitere Informationen finden Sie unter Löschen von Benachrichtigungskontakten. Sie können einen Alarm auch deaktivieren oder löschen, wenn Sie keine Benachrichtigungen für einen bestimmten Alarm mehr erhalten möchten. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen.

Zustandsmetriken für Lightsail Load Balancer anzeigen

Nachdem Sie einen Load Balancer in Amazon Lightsail erstellt und ihm Instances angefügt haben, können Sie die Metrikdiagramme auf der Registerkarte „Metriken“ der Verwaltungsseite

der Lastenverteilung anzeigen. Die Überwachung von Metriken ist ein wichtiger Teil, um die Zuverlässigkeit, Verfügbarkeit und Performance Ihrer Ressourcen aufrechtzuerhalten. Überwachen und sammeln Sie regelmäßig Metrikdaten von Ihren Ressourcen, damit Sie bei Auftreten eines Mehrpunkt-Fehlers diesen leichter debuggen können. Weitere Informationen zu Metriken finden Sie unter Metriken.

Bei der Überwachung Ihrer Ressourcen sollten Sie einen Bereich für die normale Ressourcenleistung in Ihrer Umgebung festlegen. Nachdem Sie einen Grundwert erstellt haben, können Sie in der Lightsail-Konsole Alarme konfigurieren, damit Sie benachrichtigt werden, wenn Ihre Ressourcen außerhalb der festgelegten Schwellenwerte arbeiten. Weitere Informationen finden Sie unter Benachrichtigungen und Alarme.

Inhalt

Load Balancer-Metriken

Die folgenden Load Balancer-Metriken sind verfügbar:

- Fehlerfreie Hostanzahl (**`HealthyHostCount`**) – Die Anzahl der Ziel-Instances, die als fehlerfrei betrachtet werden.
- Anzahl fehlerhafter Hosts (**`UnhealthyHostCount`**) – Die Anzahl der Ziel-Instances, die als fehlerhaft betrachtet werden.
- Load Balancer HTTP-4XX (**`HTTPCode_LB_4XX_Count`**) – Anzahl von HTTP-4XX-Client-Fehlercodes, die von Load Balancern verursacht werden. Client-Fehler werden bei Anforderungen mit falschem Format oder unvollständigen Anforderungen generiert. Diese Anforderungen wurden von der Ziel-Instance nicht empfangen. Diese Anzahl umfasst keine Antwortcodes, die von den Ziel-Instances generiert wurden.
- Load Balancer-HTTP-5XX (**`HTTPCode_LB_5XX_Count`**) – Anzahl von HTTP-5XX-Server-Fehlercodes, die von Load Balancern verursacht werden. Hierin sind keine von der Ziel-Instance generierten Antwortcodes enthalten. Die Metrik wird gemeldet, wenn für den Load Balancer keine fehlerfreien Instances angefügt sind oder wenn die Anforderungsrate die Kapazität der Instances (Überlauf) oder des Load Balancers überschreitet.

- HTTP-2XX-Instance (**`HTTPCode_Instance_2XX_Count`**) – Die Anzahl der HTTP-2XX-Antwortcodes, die von den Ziel-Instances generiert werden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.
- HTTP-3XX-Instance (**`HTTPCode_Instance_3XX_Count`**) – Die Anzahl der HTTP-3XX-Antwortcodes, die von den Ziel-Instances generiert werden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.
- HTTP-4XX-Instance (**`HTTPCode_Instance_4XX_Count`**) – Die Anzahl der HTTP-4XX-Antwortcodes, die von den Ziel-Instances generiert werden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.
- HTTP-5XX-Instance (**`HTTPCode_Instance_5XX_Count`**) – Die Anzahl der HTTP-5XX-Antwortcodes, die von den Ziel-Instances generiert werden. Hierin sind keine vom Load Balancer generierten Antwortcodes enthalten.
- Instance-Antwortzeit (**`InstanceResponseTime`**) – Die verstrichene Zeit in Sekunden bis zum Empfang einer Antwort von der Ziel-Instance, nachdem die Anforderung den Load Balancer verlassen hat.
- Fehlerzahl-Client-TLS-Vereinbarung (**`ClientTLSNegotiationErrorCount`**) – Die Anzahl der vom Client initiierten TLS-Verbindungen, die keine Sitzung mit de Load Balancer eingerichtet haben, da der Load Balancer einen TLS-Fehler generiert hat. Als mögliche Ursachen kommen unter anderem fehlende Übereinstimmung bei Verschlüsselungsverfahren oder Protokollen infrage.
- Anzahl der Anforderungen (**`RequestCount`**) – Die Anzahl von Anforderungen, die über IPv4 verarbeitet wurden. In dieser Zahl sind nur die Anforderungen mit einer Antwort enthalten, die von einer Ziel-Instance des Load Balancers generiert wurden.
- Anzahl der abgelehnten Verbindungen (**`RejectedConnectionCount`**) Die Anzahl der abgelehnten Verbindungen, weil der Load Balancer die maximale Anzahl an Verbindungen erreicht hat.

Load Balancer-Metriken

Führen Sie die folgenden Schritte aus, um Load Balancer-Metriken in der Lightsail-Konsole anzuzeigen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen des Load Balancers, für den Sie sich die Metriken anzeigen lassen möchten.

4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Seite „Load Balancer Management“.
5. Wählen Sie die Metrik aus, die Sie im Dropdown-Menü unter der Überschrift Metrics graphs (Metrikdiagramme) anzeigen möchten.

   Das Diagramm zeigt eine visuelle Darstellung der Datenpunkte für die gewählte Metrik an.
6. Im Metrikdiagramm können Sie die folgenden Aktionen ausführen:

   - Sie können die Ansicht des Diagramms ändern, um Daten für 1 Stunde, 6 Stunden, 1 Tag, 1 Woche und 2 Wochen anzuzeigen.
   - Sie können den Cursor auf einem Datenpunkt anhalten, um detaillierte Informationen zu diesem Datenpunkt anzuzeigen.
   - Sie können einen Alarm für die ausgewählte Metrik hinzufügen, damit Sie benachrichtigt werden, wenn die Metrik einen von Ihnen angegebenen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Alarme und Erstellen von Load Balancer-Metrikalarmen.

Nächste Schritte

Es gibt einige zusätzliche Aufgaben, die Sie für Ihre Load Balancer-Metriken ausführen können:

- Sie können einen Alarm für die ausgewählte Metrik hinzufügen, damit Sie benachrichtigt werden, wenn die Metrik einen von Ihnen angegebenen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Alarme und Erstellen von Load Balancer-Metrikalarmen.
- Wenn ein Alarm ausgelöst wird, wird ein Benachrichtigungsbanner in der Lightsail-Konsole angezeigt. Um per E-Mail und SMS benachrichtigt zu werden, müssen Sie in jeder AWS-Region, in der Sie Ihre Ressourcen überwachen möchten, Ihre E-Mail-Adresse und Mobiltelefonnummer als Benachrichtigungskontakt angeben. Weitere Informationen finden Sie unter Hinzufügen von Benachrichtigungskontakten.
- Wenn Sie keine Benachrichtigungen mehr erhalten möchten, können Sie Ihre E-Mail und Ihre Mobiltelefonnummer aus Lightsail entfernen. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen. Sie können einen Alarm auch deaktivieren oder löschen, wenn Sie keine Benachrichtigungen für einen bestimmten Alarm mehr erhalten möchten. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen.

Themen

- Metrikalarme für Lightsail-Load-Balancer erstellen

Metrikalarme für Lightsail-Load-Balancer erstellen

Sie können einen Amazon Lightsail-Alarm erstellen, der eine einzelne Load Balancer-Metrik überwacht. Ein Alarm kann so konfiguriert werden, dass Sie basierend auf dem Wert der Metrik relativ zu einem von Ihnen angegebenen Schwellenwert benachrichtigt werden. Benachrichtigungen können ein in der Lightsail-Konsole angezeigtes Banner, eine an Ihre E-Mail-Adresse gesendete E-Mail oder eine an Ihre Mobiltelefonnummer gesendete SMS-Nachricht sein. Weitere Informationen über Alarme finden Sie unter Alarme.

Inhalt

Alarmgrenzen für Load Balancer

Die folgenden Limits gelten für Alarme:

- Sie können zwei Alarme pro Metrik konfigurieren.
- Alarme werden in Intervallen von 5 Minuten ausgewertet. Jeder Datenpunkt für Alarme stellt einen Zeitraum von 5 Minuten aggregierter Metrikdaten dar.
- Sie können einen Alarm so konfigurieren, dass Sie nur dann benachrichtigt werden, wenn sich der Alarmzustand in `OK` ändert, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden.
- Sie können die `OK`-Alarmbenachrichtigung nur testen, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden.
- Sie können einen Alarm so konfigurieren, dass Sie nur dann benachrichtigt werden, wenn sich der Alarmstatus in `INSUFFICIENT_DATA` ändert, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden, und wenn Sie die Option Do not evaluate the missing data (Fehlende Daten nicht auswerten) für fehlende Datenpunkte wählen.
- Sie können Benachrichtigungen nur testen, wenn sich der Alarm im OK-Zustand befindet.

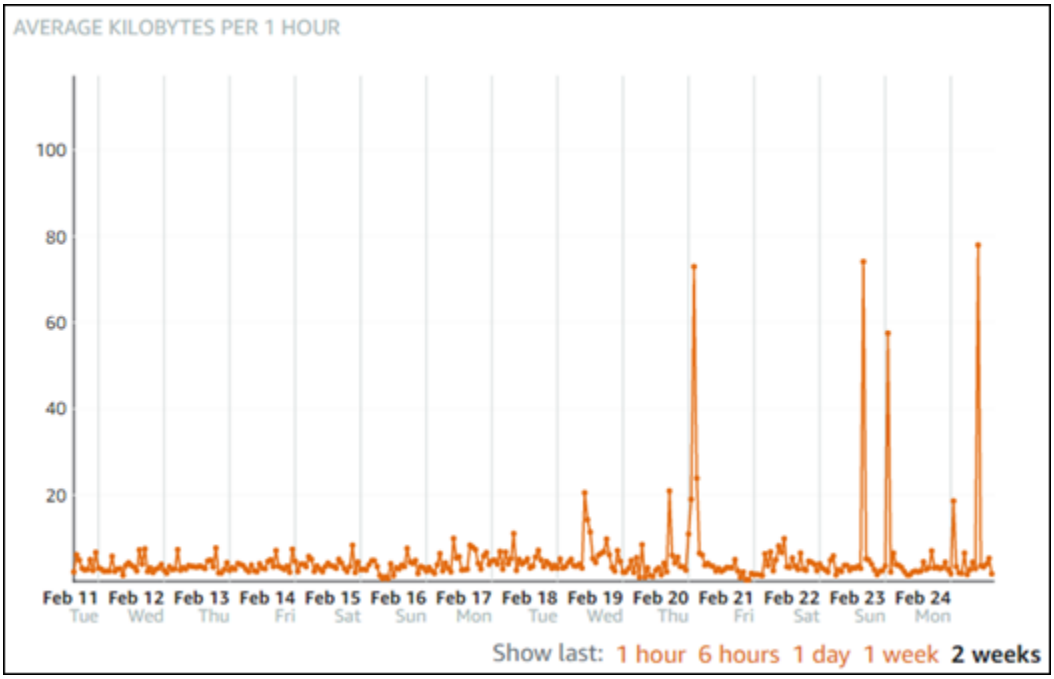
Bewährte Methoden zum Konfigurieren von Load Balancer-Alarmen

Die folgenden Limits gelten für Alarme:

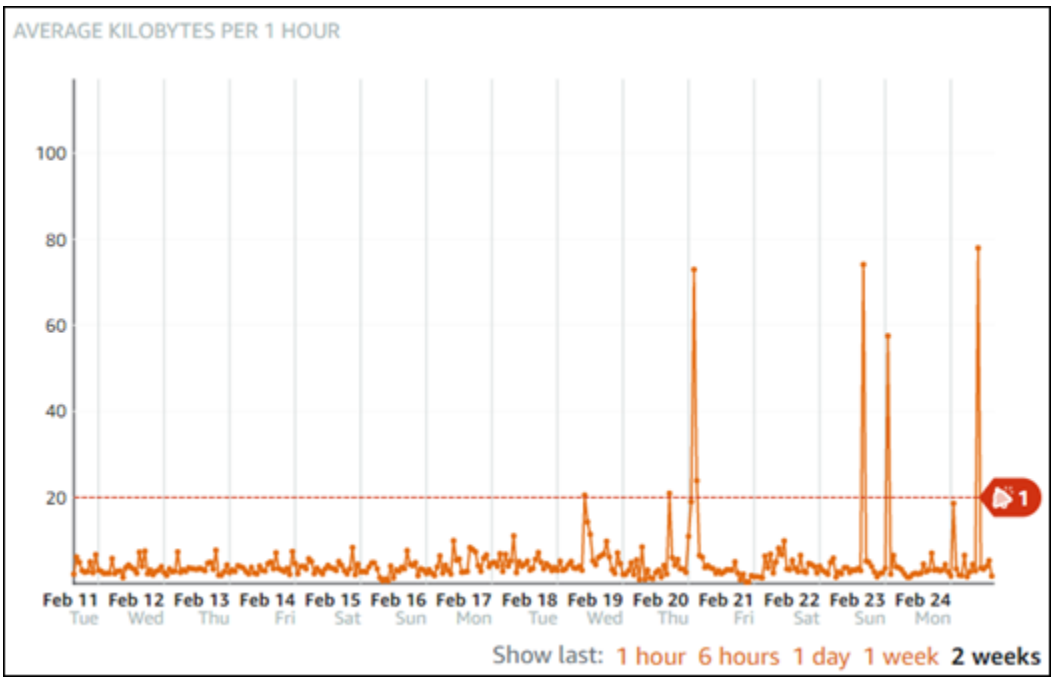
- Sie können zwei Alarme pro Metrik konfigurieren.
- Alarme werden in Intervallen von 5 Minuten ausgewertet. Jeder Datenpunkt für Alarme stellt einen Zeitraum von 5 Minuten aggregierter Metrikdaten dar.
- Sie können einen Alarm so konfigurieren, dass Sie nur dann benachrichtigt werden, wenn sich der Alarmzustand in `OK` ändert, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden.
- Sie können die `OK`-Alarmbenachrichtigung nur testen, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden.
- Sie können einen Alarm so konfigurieren, dass Sie nur dann benachrichtigt werden, wenn sich der Alarmstatus in `INSUFFICIENT_DATA` ändert, wenn Sie den Alarm so konfigurieren, dass Sie per E-Mail und/oder SMS-Textnachricht benachrichtigt werden, und wenn Sie die Option Do not evaluate the missing data (Fehlende Daten nicht auswerten) für fehlende Datenpunkte wählen.
- Sie können Benachrichtigungen nur testen, wenn sich der Alarm im OK-Zustand befindet.

Standardalarmeinstellungen

Bevor Sie einen Metrikalarm konfigurieren, sollten Sie die historischen Daten der Metrik anzeigen. Ermitteln Sie das niedrige, mittlere und hohe Niveau der Metrik im Zeitraum der letzten beiden Wochen. Im folgenden Beispiel eines Metrikdiagramms für ausgehenden Netzwerkverkehr einer Instance (`NetworkOut`) liegen das niedrige Niveau bei 0-10 KB pro Stunde, das mittlere Niveau zwischen 10-20 KB pro Stunde und das hohe Niveau zwischen 20-80 KB pro Stunde.



Wenn Sie den Alarmschwellenwert so konfigurieren, dass er im niedrigen Bereich (z. B. greater than or equal to (größer oder gleich) 5 KB pro Stunde) liegt, erhalten Sie häufigere und möglicherweise nicht erforderliche Alarmbenachrichtigungen. Wenn Sie den Alarmschwellenwert so konfigurieren, dass er im hohen Bereich (z. B. greater than or equal (größer oder gleich) 20 KB pro Stunde) liegt, erhalten Sie seltenere Alarmbenachrichtigungen, die allerdings genau untersucht werden müssen. Wenn Sie einen Alarm konfigurieren und aktivieren, wird im Diagramm wie im folgenden Beispiel eine Alarmlinie angezeigt, die den Schwellenwert darstellt. Die mit 1 beschriftete Alarmlinie stellt den Schwellenwert für Alarm 1 und die mit 2 beschriftete Alarmlinie den Schwellenwert für Alarm 2 dar.



Erstellen von Metrikalarmen für Load Balancer über die Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um mithilfe der Lightsail-Konsole einen Load Balancer-Metrikalarm zu erstellen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen des Load Balancers, für den Sie Alarme erstellen möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Seite „Load Balancer Management“.
5. Wählen Sie im Dropdown-Menü unter der Überschrift Metrics Graphs (Metrikdiagramme) die Metrik aus, für die Sie einen Alarm erstellen möchten. Weitere Informationen finden Sie unter Ressourcenmetriken.
6. Wählen Sie Alarm hinzufügen im Abschnitt Alarme der Seite.
7. Wählen Sie im Dropdown-Menü einen Vergleichsoperatorwert aus. Beispielwerte sind „Größer als oder gleich“, „Größer als“, „Kleiner als“ oder „Kleiner als oder gleich“.
8. Geben Sie einen Schwellenwert für den Alarm ein.
9. Geben Sie die Datenpunkte für den Alarm ein.
10. Wählen Sie die Bewertungszeiträume. Der Zeitraum kann in 5-Minuten-Schritten von 5 Minuten bis hin zu 24 Stunden angegeben werden.
11. Wählen Sie eine der folgenden Benachrichtigungsmethoden:

- E-Mail: Sie werden per E-Mail benachrichtigt, wenn sich der Alarmzustand in ALARM ändert.
- SMS-Textnachricht: Sie werden per SMS-Textnachricht benachrichtigt, wenn sich der Alarmzustand in ALARM ändert. SMS-Nachrichten werden nicht in allen AWS-Regionen unterstützt, in denen Sie Lightsail-Ressourcen erstellen können. SMS-Textnachrichten können nicht in alle Länder/Regionen gesendet werden. Weitere Informationen finden Sie unter Unterstützung von SMS-Textnachrichten.

> **Note**
>
> Sie müssen eine E-Mail-Adresse oder Mobiltelefonnummer hinzufügen, wenn Sie sich für eine Benachrichtigung per E-Mail oder SMS entscheiden, aber noch keinen Benachrichtigungskontakt in der AWS-Region der Ressource konfiguriert haben. Weitere Informationen finden Sie unter Benachrichtigungen.

12. (Optional) Wählen Sie Send me a notification when the alarm state change to OK (Benachrichtigung senden, wenn sich der Alarmzustand in OK ändert), um benachrichtigt zu werden, wenn der Alarmzustand zu OK wechselt. Diese Option ist nur verfügbar, wenn Sie per E-Mail oder SMS-Textnachricht benachrichtigt werden möchten.
13. (Optional) Wählen Sie Advanced settings (Erweiterte Einstellungen) und dann eine der folgenden Optionen:

    - Legen Sie fest, wie der Alarm fehlende Daten behandeln soll. Folgende Optionen stehen zur Verfügung:
      - Angenommen, sie liegen nicht innerhalb des zulässigen Bereichs (Schwellenwert überschritten): Fehlende Datenpunkte werden als fehlerhaft behandelt und liegen außerhalb des gültigen Bereichs.
      - Angenommen, sie liegen innerhalb des gültigen Bereichs (Schwellenwert nicht überschritten): Fehlende Datenpunkte werden als ordnungsgemäß betrachtet und liegen innerhalb des gültigen Bereichs.
      - Den Wert des letzten gültigen Datenpunkts verwenden (Ignorieren und aktuellen Alarmzustand beibehalten) – Der aktuelle Alarmzustand wird beibehalten.
      - Nicht bewerten (Fehlende Daten als fehlend Daten behandeln): Bei der Bewertung, ob der Status geändert werden soll, werden fehlende Datenpunkte nicht berücksichtigt.
    - Wählen Sie Send a notification if there is insufficient data (Benachrichtigung senden, wenn nicht genügend Daten vorhanden) sind, um benachrichtigt zu werden, wenn der Alarmzustand

in INSUFFICIENT_DATA geändert wird. Diese Option ist nur verfügbar, wenn Sie per E-Mail oder SMS-Textnachricht benachrichtigt werden möchten.

14. Wählen Sie Create (Erstellen), um den Alarm hinzuzufügen.

    Um den Alarm später zu bearbeiten, wählen Sie das Ellipsensymbol (⋮) neben dem Alarm, den Sie bearbeiten möchten, und wählen Sie Alarm bearbeiten.

Testen von Metrikalarmen für Load Balancer über die Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um einen Alarm über die Lightsail-Konsole zu testen. Sie können einen Alarm testen, um zu bestätigen, dass die konfigurierten Benachrichtigungsoptionen funktionieren, um beispielsweise sicherzustellen, dass Sie bei Auslösung des Alarms eine E-Mail oder eine SMS-Textnachricht erhalten.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wechseln Sie auf der Lightsail-Startseite zur Registerkarte Netzwerk.
3. Wählen Sie den Namen des Load Balancers, für den Sie einen Alarm testen möchten.
4. Wählen Sie die Registerkarte Metrics (Metriken) auf der Seite „Load Balancer Management“.
5. Wählen Sie im Dropdown-Menü unter der Überschrift Metrics Graphs (Metrikdiagramme) die Metrik aus, für die Sie einen Alarm testen möchten.
6. Scrollen Sie nach unten zum Abschnitt Alarme und wählen Sie neben dem zu testenden Alarm das Ellipsensymbol (⋮) aus.
7. Wählen Sie eine der folgenden Optionen:

    - Alarmbenachrichtigung testen – Wählen Sie diese Option, um die Benachrichtigungen zu testen, wenn sich der Alarmstatus zu `ALARM` ändert.
    - OK-Benachrichtigung testen – Wählen Sie diese Option, um die Benachrichtigungen zu testen, wenn sich der Alarmstatus zu `OK` ändert.

> **Note**
>
> Wenn eine dieser Optionen nicht verfügbar ist, haben Sie die Benachrichtigungsoptionen für den Alarm möglicherweise nicht konfiguriert, oder der Alarm befindet sich derzeit in einem `ALARM`-Zustand. Weitere Informationen finden Sie unter Alarmgrenzen für Load Balancer.

Der Alarm ändert sich je nach ausgewählter Testoption vorübergehend in den Zustand `OK` oder `ALARM`, und je nachdem, was Sie als Benachrichtigungsmethode für den Alarm konfiguriert haben, wird eine E-Mail und/oder SMS-Textnachricht gesendet. Ein Benachrichtigungsbanner wird nur dann in der Lightsail-Konsole angezeigt, wenn Sie die `ALARM`-Benachrichtigung testen möchten. Ein Benachrichtigungsbanner wird nicht angezeigt, wenn Sie die `OK`-Benachrichtigung testen möchten. Der Alarm kehrt oft nach einigen Sekunden in seinen tatsächlichen Zustand zurück.

Nächste Schritte nach dem Erstellen von Load Balancer-Alarmen

Es gibt einige zusätzliche Aufgaben, die Sie für Ihre Load Balancer-Alarme ausführen können:

- Wenn Sie keine Benachrichtigungen mehr erhalten möchten, können Sie Ihre E-Mail und Ihre Mobiltelefonnummer aus Lightsail entfernen. Weitere Informationen finden Sie unter Löschen von Benachrichtigungskontakten. Sie können einen Alarm auch deaktivieren oder löschen, wenn Sie keine Benachrichtigungen für einen bestimmten Alarm mehr erhalten möchten. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen.

Hinzufügen von Benachrichtigungskontakten in Lightsail

Sie können Amazon Lightsail so konfigurieren, dass Sie benachrichtigt werden, wenn eine Metrik für eine Ihrer Instances, Datenbanken, Load Balancer oder Bereitstellung von Inhalten Ihres Netzwerks (CDN) einen angegebenen Schwellenwert überschreitet. Benachrichtigungen können in Form eines Banners, das auf der Lightsail-Konsole angezeigt wird, einer E-Mail an eine von Ihnen angegebene Adresse oder einer SMS-Textnachricht an eine von Ihnen angegebene Mobiltelefonnummer erfolgen. Um per E-Mail und SMS benachrichtigt zu werden, müssen Sie in jeder AWS-Region, in der Sie Ihre Ressourcen überwachen möchten, Ihre E-Mail-Adresse und Mobiltelefonnummer als Benachrichtigungskontakt angeben. Weitere Informationen zu Benachrichtigungen finden Sie unter Benachrichtigungen.

> **Important**
>
> Das SMS-Textnachrichten-Feature wurde vorübergehend deaktiviert und wird derzeit in keiner AWS-Region unterstützt, in der Sie Lightsail-Ressourcen erstellen können. Weitere Informationen finden Sie unter Unterstützung von SMS-Textnachrichten.

Inhalt

Regionale Begrenzungen für Benachrichtigungskontakte

Sie können in jeder AWS-Region nur eine E-Mail-Adresse und eine Mobiltelefonnummer hinzufügen. Wenn Sie eine E-Mail-Adresse oder Mobiltelefonnummer in einer Region hinzufügen, in der diese bereits hinzugefügt wurden, werden Sie gefragt, ob Sie den vorhandenen Benachrichtigungskontakt durch den neuen Kontakt ersetzen möchten.

Wenn Sie mehrere E-Mail-Empfänger in einer AWS-Region benötigen, können Sie eine Verteilerliste konfigurieren, die an mehrere Empfänger weitergeleitet wird, und die E-Mail-Adresse der Verteilerliste als Benachrichtigungskontakt hinzufügen.

Unterstützung für SMS-Textnachrichten

> **Important**
>
> Das SMS-Textnachrichten-Feature wurde vorübergehend deaktiviert und wird derzeit in keiner AWS-Region unterstützt, in der Sie Lightsail-Ressourcen erstellen können. Alternativ können Sie E-Mail-Nachrichten konfigurieren oder sich auf die in der Lightsail-Konsole angezeigten Benachrichtigungsbanner beziehen.
> Die folgenden Informationen zur Unterstützung von SMS-Textnachrichten werden für Kunden veröffentlicht, die SMS-Textnachrichten konfiguriert haben, bevor wir die Feature deaktiviert haben.

SMS-Textnachrichten werden nicht in allen AWS-Regionen unterstützt, in denen Sie Lightsail-Ressourcen erstellen können. Außerdem können SMS-Textnachrichten in einige Länder und Regionen der Welt nicht gesendet werden. Für AWS-Regionen, in denen SMS-Nachrichten nicht unterstützt werden, können Sie nur einen E-Mail-Benachrichtigungskontakt konfigurieren.

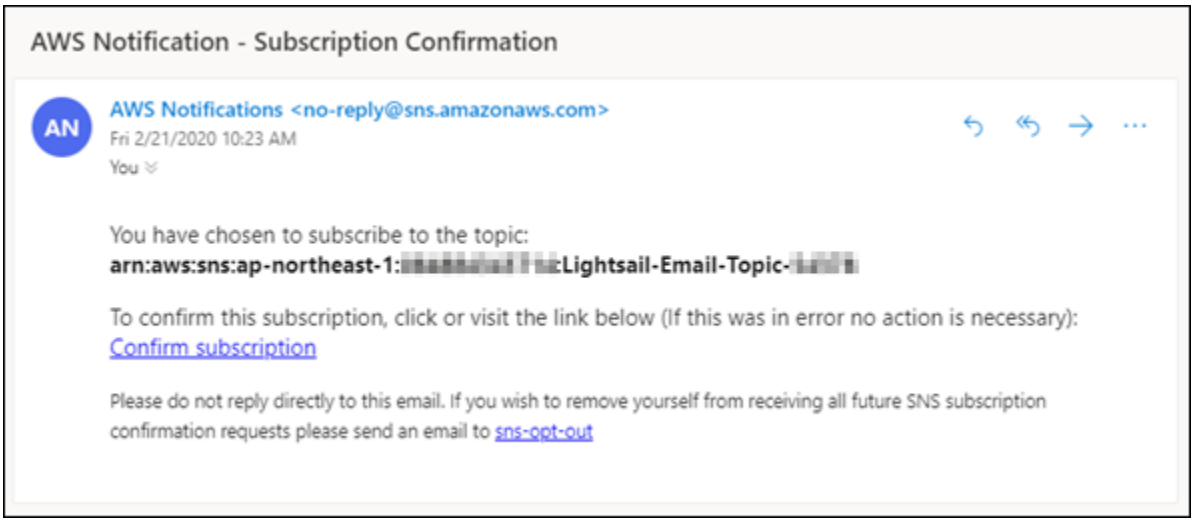
SMS-Nachrichten werden in den folgenden AWS-Regionen unterstützt. Dies sind Regionen, in denen SMS-Textnachrichten vom Amazon Simple Notification Service (Amazon SNS) unterstützt wird, der von Lightsail verwendet wird, um Ihnen Benachrichtigungen zu senden:

- USA Ost (Nord-Virginia): (us-east-1)
- USA West (Oregon): (us-west-2)
- Asien-Pazifik (Singapur): (ap-southeast-1)
- Asien-Pazifik (Sydney): (ap-southeast-2)
- Asien-Pazifik (Tokyo) (ap-northeast-1)
- Europa (Irland) (eu-west-1)

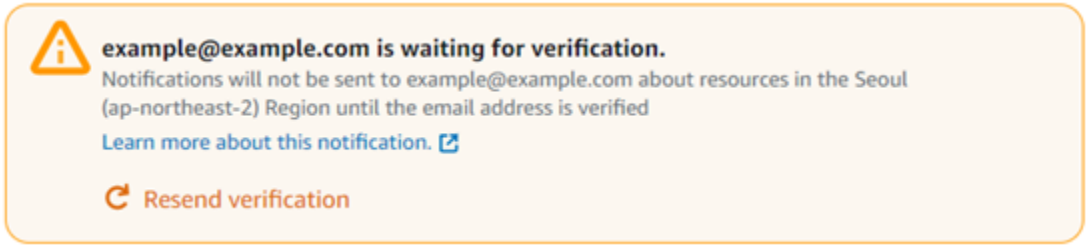
Eine Liste der Länder und Regionen der Welt, in denen SMS-Text-Messaging gesendet werden kann, sowie die neuesten AWS-Regionen, in denen SMS-Text-Messaging unterstützt wird, finden Sie unter Unterstützte Regionen und Länder im Entwicklerhandbuch von Amazon SNS.

Verifizierung von E-Mail-Kontakten

Wenn Sie eine E-Mail-Adresse als Benachrichtigungskontakt in Lightsail hinzufügen, wird eine Verifizierungsanfrage an diese Adresse gesendet. Die Bestätigungs-E-Mail enthält einen Link, auf den der Empfänger klicken muss, um den gewünschten Erhalt von Lightsail-Benachrichtigungen zu bestätigen. Benachrichtigungen werden erst nach der Verifizierung an die E-Mail-Adresse gesendet. Die Verifizierung erhalten Sie von AWS-Benachrichtigungen <no-reply@sns.amazonaws.com> und der Betreff lautet AWS-Benachrichtigung-Abonnement-Bestätigung. Für SMS-Nachrichten ist keine Verifizierung erforderlich.



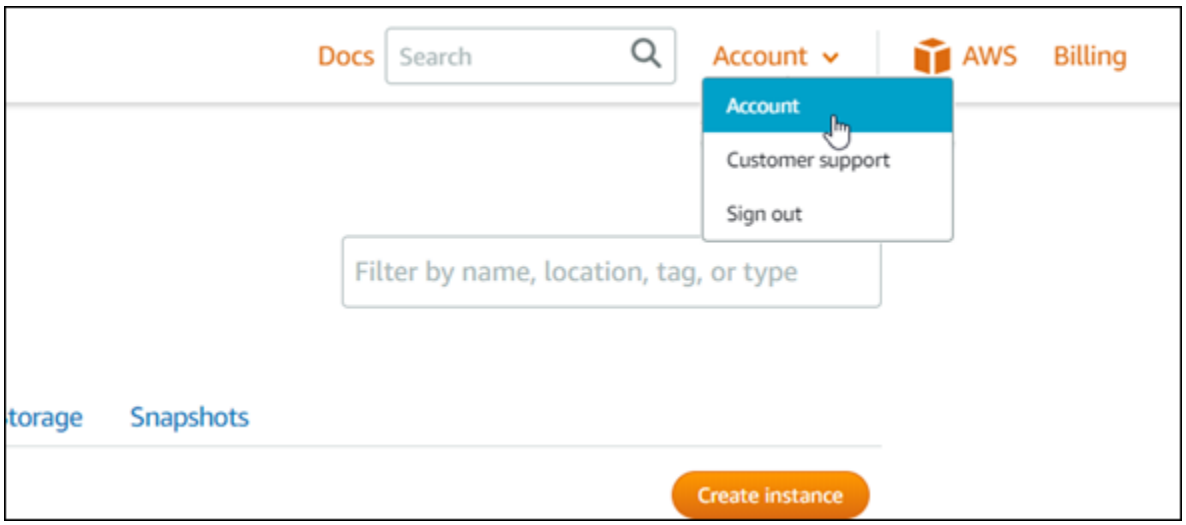
Überprüfen Sie die Spam- und Junk-Ordner des Postfachs, wenn sich die Bestätigungs-E-Mail nicht im Posteingang befindet. Wenn die Verifizierungsanforderung verloren gegangen ist oder gelöscht wurde, wählen Sie Verifizierung erneut senden im Benachrichtigungsbanner, das in der Lightsail-Konsole und in der Seite Kontoangezeigt wird.



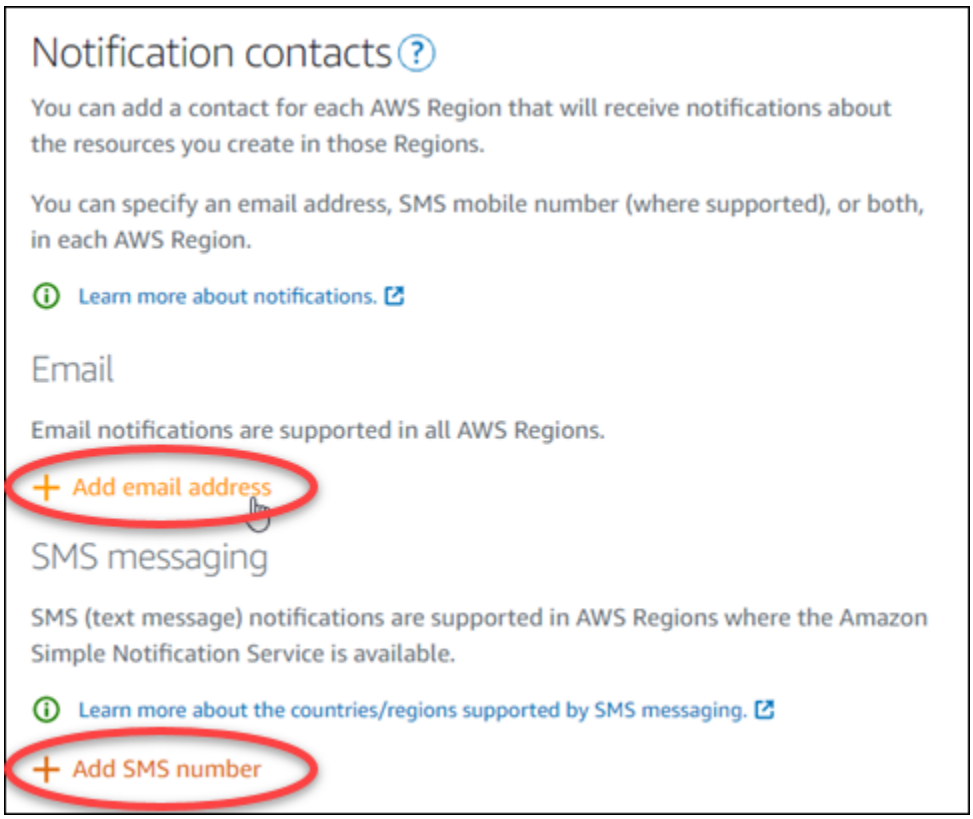
Hinzufügen von Benachrichtigungskontakten über die Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um Benachrichtigungskontakte über die Lightsail-Konsole hinzuzufügen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite im oberen Navigationsmenü Account (Konto) aus.
3. Wählen Sie im Dropdownmenü Account (Konto) aus.

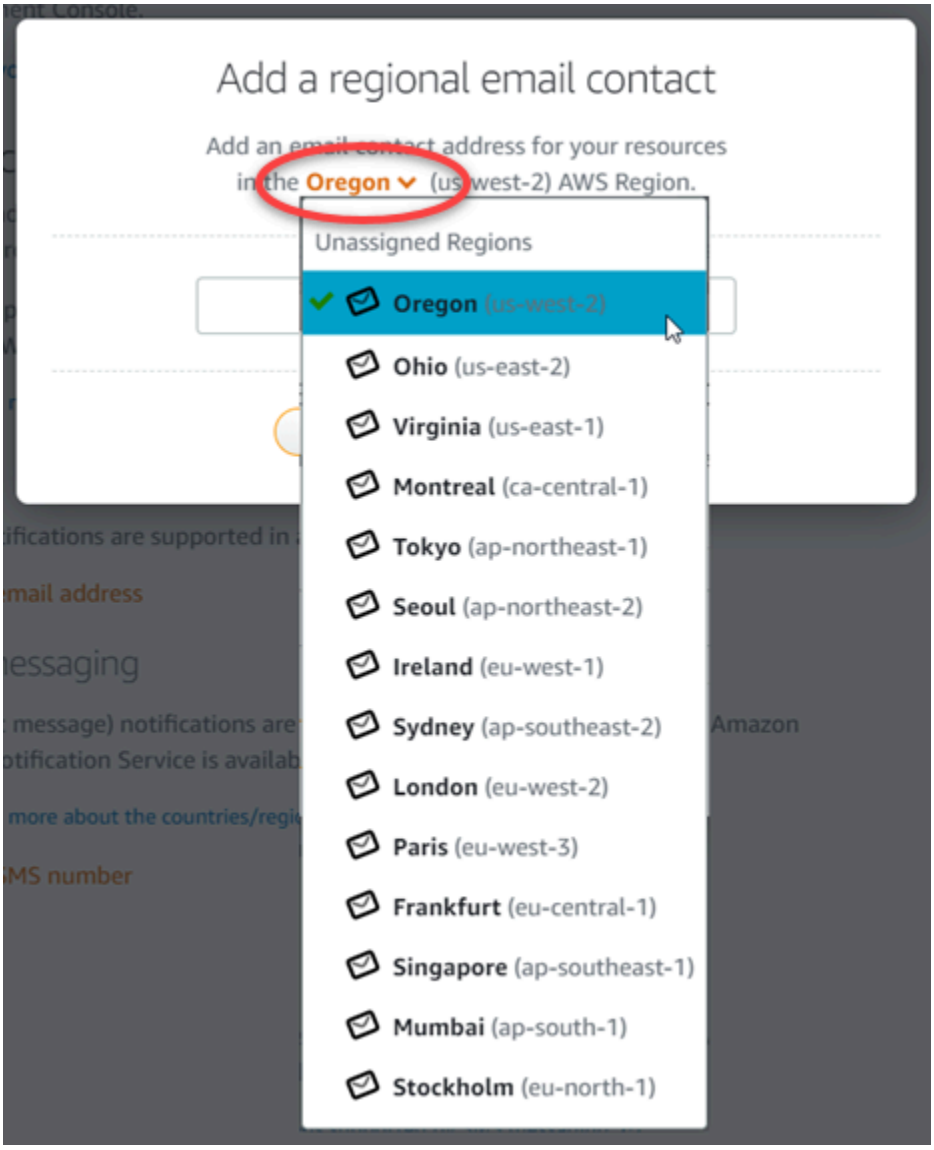


4. Wählen Sie E-Mail-Adresse hinzufügen oder SMS-Nummer hinzufügen im Abschnitt Benachrichtigungskontakte auf der Registerkarte Profile und Kontakte aus.



5. Führen Sie die folgenden Schritte aus:

   - Wenn Sie eine E-Mail-Adresse hinzufügen, wählen Sie die AWS-Region aus, in der Sie den Benachrichtigungskontakt hinzufügen möchten. Geben Sie Ihre E-Mail-Adresse in das Textfeld ein.

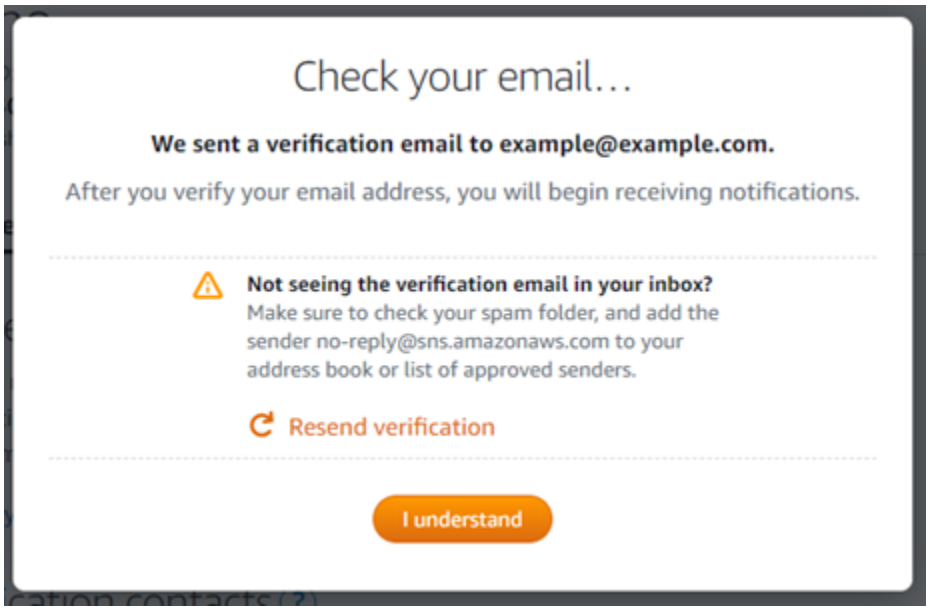


- Wenn Sie eine SMS-Nummer hinzufügen, wählen Sie die AWS-Region aus, in der Sie den Benachrichtigungskontakt hinzufügen möchten. Wählen Sie das Land Ihrer Mobilnummer aus und geben Sie es in das Textfeld ein. Der Ländercode ist bereits für Sie eingetragen.

> **Important**
>
> Das SMS-Textnachrichten-Feature wurde vorübergehend deaktiviert und wird derzeit in keiner AWS-Region unterstützt, in der Sie Lightsail-Ressourcen erstellen können. Weitere Informationen finden Sie unter Unterstützung von SMS-Textnachrichten.

6. Wählen Sie Add Contact (Kontakt hinzufügen).

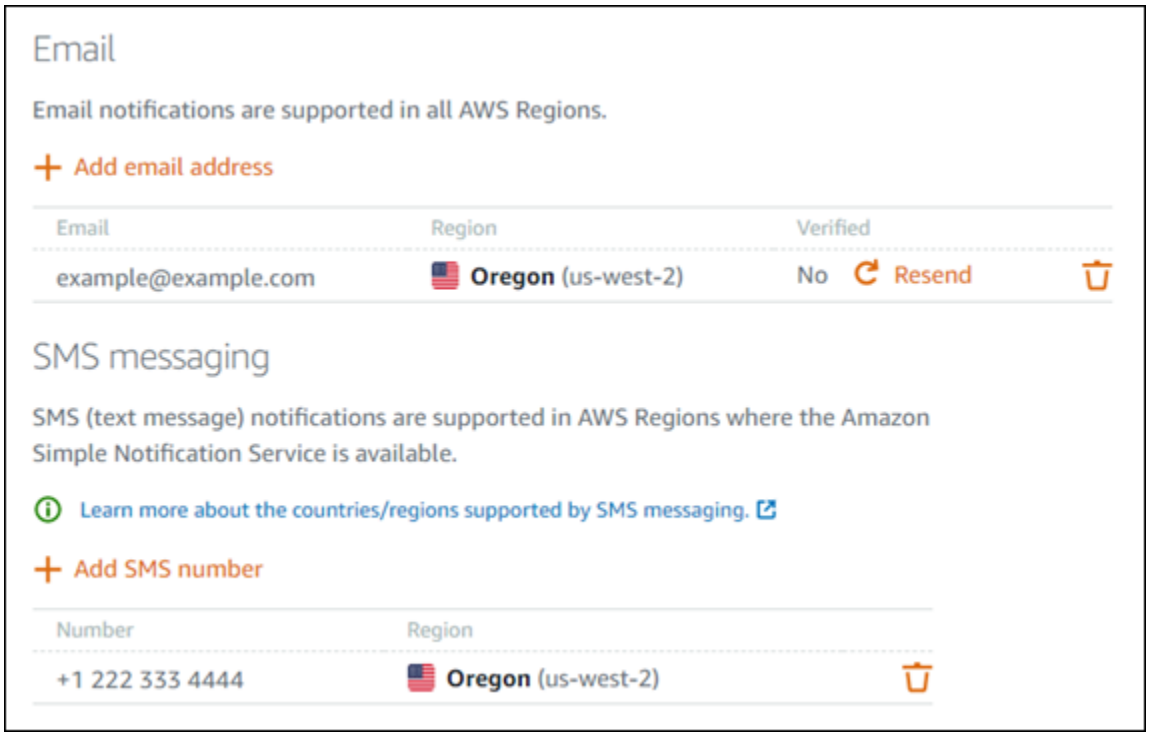
   Bei Hinzufügen einer E-Mail-Adresse als Benachrichtigungskontakt wird eine Verifizierungsanfrage an diese Adresse gesendet. Die Bestätigungs-E-Mail enthält einen Link, auf den der Empfänger klicken muss, um den gewünschten Erhalt von Lightsail-Benachrichtigungen zu bestätigen. Für SMS-Nachrichten ist keine Verifizierung erforderlich.



7. Wählen Sie I understand (Ich verstehe).

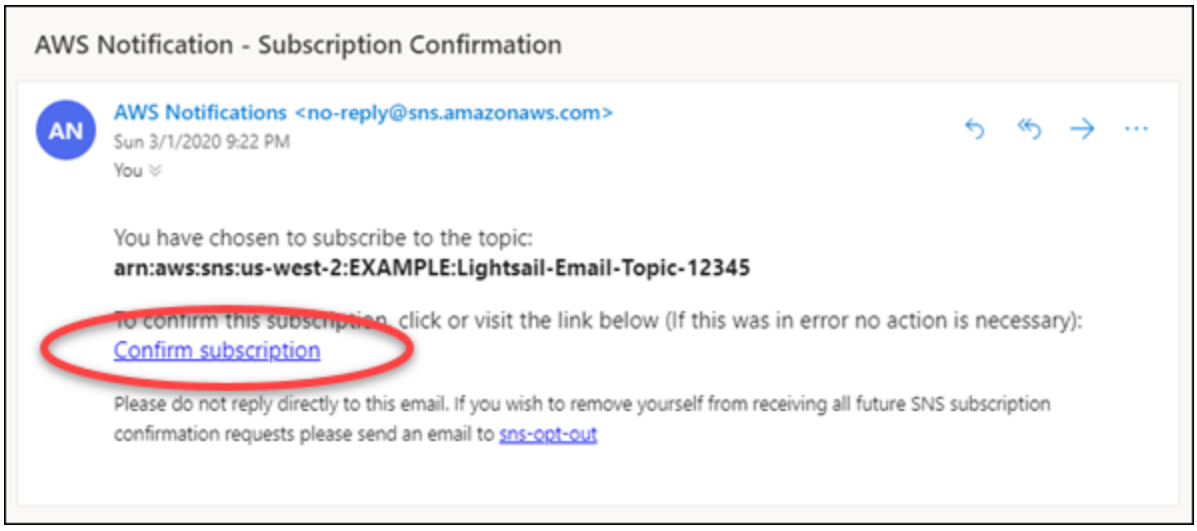
Ihre E-Mail-Adresse oder Mobiltelefonnummer wird dem Abschnitt Notification contacts (Benachrichtigungskontakte) hinzugefügt. E-Mail-Adressen werden erst überprüft, wenn Sie den Verifizierungsprozess in den folgenden Schritten abgeschlossen haben. Benachrichtigungen werden erst nach der Verifizierung an die E-Mail-Adresse gesendet. Wählen Sie neben einer Ihrer regionalen E-Mail-Adressen Resend (Erneut senden), um eine weitere Verifizierungsanfrage zu senden, falls die Verifizierungsanfrage verloren gegangen ist oder gelöscht wurde.

> **Note**
>
> Für SMS-Nachrichten ist keine Verifizierung erforderlich. Daher müssen Sie die Schritte 8 bis 10 in diesem Verfahren nicht ausführen, nachdem Sie einen SMS-Benachrichtigungskontakt hinzugefügt haben.



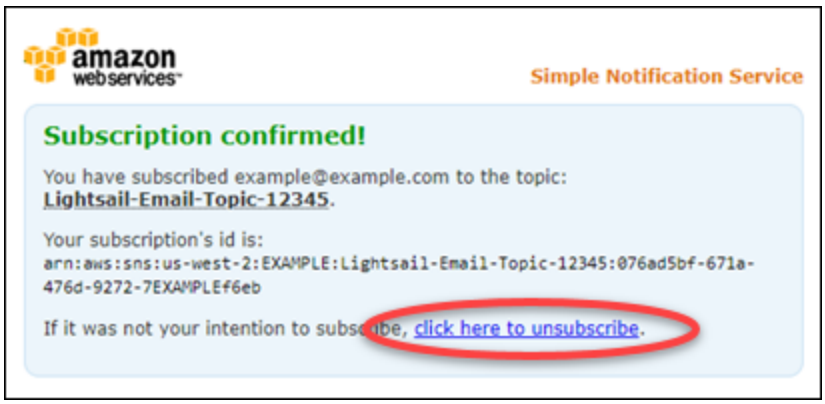
8. Öffnen Sie den Posteingang für die E-Mail-Adresse, die Sie als Benachrichtigungskontakt in Lightsail hinzugefügt haben.
9. Öffnen Sie die E-Mail AWS-Benachrichtigung – Abonnementbestätigung von no-reply@sns.amazonaws.com.

> **Note**
>
> Überprüfen Sie die Spam- und Junk-Ordner des Postfachs, wenn sich die Bestätigungs-E-Mail nicht im Posteingang befindet.



10. Wählen Sie Confirm subscription (Abonnement bestätigen) in der E-Mail aus, um zu bestätigen, dass Sie Lightsail-Benachrichtigungen erhalten möchten.

    Ein Browserfenster öffnet sich auf der folgenden Seite, auf der Ihr Abonnement bestätigt wird. Click here to unsubscribe (Zum Kündigen klicken Sie hier) auf der Seite. Wenn Sie die Seite geschlossen haben, führen Sie die Schritte aus, um Ihre Benachrichtigungskontakte zu löschen.



Hinzufügen von Benachrichtigungskontakten mithilfe der AWS CLI

Führen Sie die folgenden Schritte aus, um Benachrichtigungskontakte für Lightsail mithilfe der AWS Command Line Interface (AWS CLI) hinzuzufügen.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.

   Falls noch nicht geschehen, installieren Sie die AWS CLI und konfigurieren Sie sie so, dass sie mit Lightsail funktioniert.

2. Geben Sie den folgenden Befehl ein, um einen Benachrichtigungskontakt hinzuzufügen:

   ```
   aws lightsail create-contact-method --region Region --notificationProtocol Protocol
    --contact-endpoint Destination
   ```

   Ersetzen Sie im Befehl Folgendes:

   - *Region* mit der AWS-Region, in der der Benachrichtigungskontakt hinzugefügt werden soll.
   - *Protocol* durch das Benachrichtigungsprotokoll für den Kontakt, das E-Mail oder SMS lauten muss.
   - *Destination* durch die E-Mail-Adresse oder Mobiltelefonnummer.

     > **Note**
     >
     > Verwenden Sie das E.164-Format, wenn Sie eine Mobiltelefonnummer angeben. Die Richtlinie E.164 legt die internationale Schreibweise für Telefonnummern fest. Telefonnummern in diesem Format bestehen aus maximal 15 Zeichen sowie einem vorangestellten Plus-Zeichen (+) und der Ländervorwahl. Eine US-Telefonnummer im E.164-Format ist beispielsweise wie folgt angegeben: +1XXX5550100. Weitere Informationen finden Sie unter E.164 in Wikipedia.

   Beispiele:

   ```
   aws lightsail create-contact-method --region us-west-2 --notificationProtocol Email
    --contact-endpoint example@example.com
   ```

```
aws lightsail create-contact-method --region us-east-1 --notificationProtocol SMS
 --contact-endpoint +14445556666
```

Wenn Sie die Eingabetaste drücken, erhalten Sie eine Information zum Vorgang mit Details zu Ihrer Anfrage.

Eine Verifizierungsanfrage wird an die E-Mail-Adresse gesendet, die Sie als Benachrichtigungskontakt angegeben haben. Dadurch wird bestätigt, dass der Empfänger Lightsail-Benachrichtigungen abonnieren möchte. E-Mail-Adressen werden erst überprüft, wenn Sie den Verifizierungsprozess in den folgenden Schritten abgeschlossen haben. Benachrichtigungen werden erst nach der Verifizierung der E-Mail-Adresse an diese gesendet. Wählen Sie neben einer Ihrer regionalen E-Mail-Adressen Resend (Erneut senden), um eine weitere Verifizierungsanfrage zu senden, falls die ursprüngliche Benachrichtigung falsch platziert wurde.

> **Note**
>
> Für SMS-Nachrichten ist keine Verifizierung erforderlich. Daher müssen Sie die Schritte 8 bis 10 in diesem Verfahren nicht ausführen, wenn Sie einen SMS-Benachrichtigungskontakt hinzugefügt haben.

3. Öffnen Sie den Posteingang für die E-Mail-Adresse, die Sie als Benachrichtigungskontakt hinzugefügt haben.
4. Öffnen Sie die E-Mail AWS-Benachrichtigung – Abonnementbestätigung von no-reply@sns.amazonaws.com.
5. Wählen Sie Confirm subscription (Abonnement bestätigen) in der E-Mail aus, um zu bestätigen, dass Sie E-Mail-Benachrichtigungen von Lightsail erhalten möchten.

   Ein Browserfenster öffnet sich auf der folgenden Seite, auf der Ihr Abonnement bestätigt wird. Click here to unsubscribe (Zum Kündigen klicken Sie hier) auf der Seite. Wenn Sie die Seite geschlossen haben, führen Sie die Schritte aus, um Ihre Benachrichtigungskontakte zu löschen.

Nächste Schritte nach dem Hinzufügen Ihrer Benachrichtigungskontakte

Sie können eine Reihe zusätzlicher Aufgaben für Ihre Benachrichtigungskontakte ausführen:

- Fügen Sie einen Alarm in der AWS-Region hinzu, in der Sie Ihre Benachrichtigungskontakte hinzugefügt haben. Sie können wählen, ob Sie per E-Mail und SMS-Textnachricht benachrichtigt werden, wenn der Alarm gestartet wird. Weitere Informationen finden Sie unter -Alarme.
- Wenn Sie wider Erwarten keine Benachrichtigungen erhalten, müssen Sie einige Punkte überprüfen, um sicherzustellen, dass Ihre Benachrichtigungskontakte korrekt konfiguriert sind. Weitere Informationen finden Sie unter Fehlerbehebung bei Benachrichtigungen.
- Wenn Sie keine Benachrichtigungen mehr erhalten möchten, können Sie Ihre E-Mail und Ihre Mobiltelefonnummer aus Lightsail entfernen. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen. Sie können einen Alarm auch deaktivieren oder löschen, wenn Sie keine Benachrichtigungen für einen bestimmten Alarm mehr erhalten möchten. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen.

Löschen von Lightsail-Benachrichtigungskontakten

Löschen Sie die Benachrichtigungskontakte für E-Mail-Adresse und Mobiltelefonnummer aus Amazon Lightsail, wenn Sie keine E-Mail- und SMS-Benachrichtigungen mehr für Ihre Lightsail-Ressourcen erhalten möchten. Weitere Informationen zu Benachrichtigungen finden Sie unter Benachrichtigungen.

Sie können einen Alarm auch deaktivieren oder löschen, wenn Sie keine Benachrichtigungen für einen bestimmten Alarm erhalten möchten. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen.

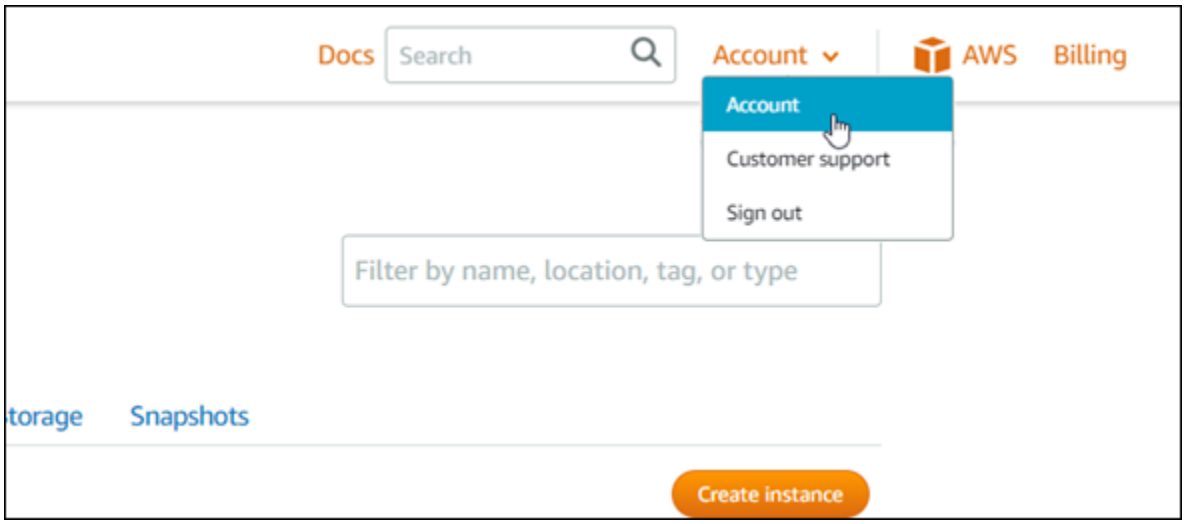
Inhalt

Löschen von Benachrichtigungskontakten über die Lightsail-Konsole

Führen Sie die folgenden Schritte aus, um Benachrichtigungskontakte über die Lightsail-Konsole zu löschen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite im oberen Navigationsmenü Account (Konto) aus.

3. Wählen Sie im Dropdownmenü Account (Konto) aus.



4. Wählen Sie im Abschnitt Notificatiion contacts (Benachrichtigungskontakte) auf der Registerkarte Profile & contacts (Profil und Kontakte) das Löschsymbol neben der E-Mail-Adresse oder Mobiltelefonnummer, die Sie löschen möchten.
5. Wählen Sie Yes (Ja), um zu bestätigen, dass Sie den Benachrichtigungskontakt löschen möchten.

Löschen von Benachrichtigungskontakten mithilfe des AWS CLI

Führen Sie die folgenden Schritte aus, um Benachrichtigungskontakte für Lightsail mithilfe des AWS Command Line Interface (AWS CLI) zu löschen.

1. Öffnen Sie ein Terminal- oder Eingabeaufforderungsfenster.

   Falls noch nicht geschehen, installieren Sie die AWS CLI und konfigurieren Sie sie so, dass sie mit Lightsail funktioniert.
2. Geben Sie den folgenden Befehl ein, um einen Benachrichtigungskontakt zu löschen:

   ```
   aws lightsail delete-contact-method --region Region --notificationProtocol Protocol
   ```

   Ersetzen Sie im Befehl Folgendes:

   - Ersetzen Sie die *Region* mit der AWS-Region, in der der Benachrichtigungskontakt gelöscht werden soll.

- Ersetzen Sie das *Protokoll* mit dem Benachrichtigungsprotokoll für den Kontakt, den Sie löschen möchten, z. B. E-Mail oder SMS.

Beispiel:

```
aws lightsail delete-contact-method --region us-west-2 --notificationProtocol SMS
```

Wenn Sie die Eingabetaste drücken, erhalten Sie eine Information zum Vorgang mit Details zu Ihrer Anfrage.

Nächste Schritte nach dem Löschen Ihrer Benachrichtigungskontakte

Nach dem Löschen Ihrer Benachrichtigungskontakte können Sie eine Reihe zusätzlicher Aufgaben ausführen:

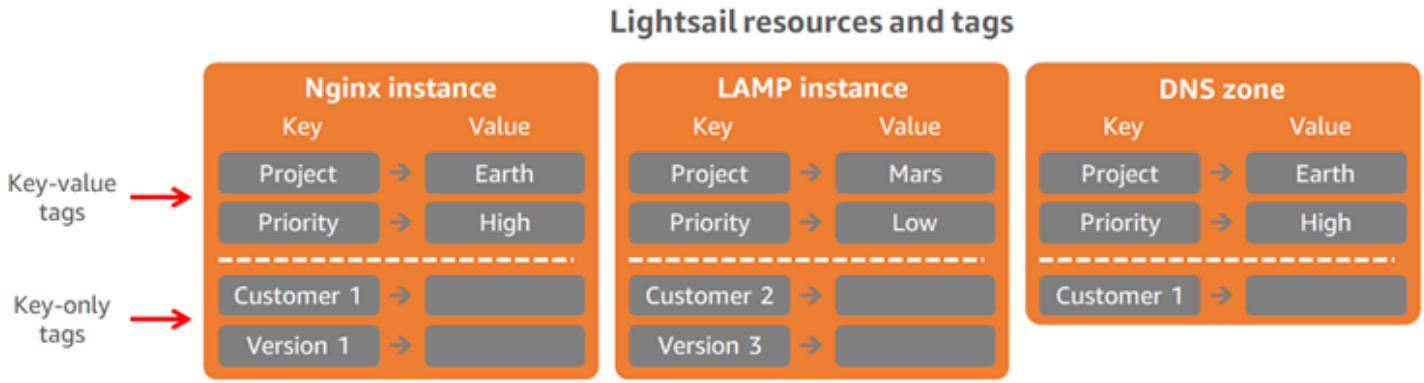
- Das Löschen von Benachrichtigungskontakten verhindert den Erhalt von E-Mail- und SMS-Benachrichtigungen, jedoch nicht die Anzeige von Benachrichtigungsbannern in der Lightsail-Konsole. Wenn Ihnen neben E-Mail- und SMS-Benachrichtigungen auch keine Benachrichtigungsbanner mehr angezeigt werden sollen, deaktivieren oder löschen Sie die Alarme, durch die sie ausgelöst werden. Weitere Informationen finden Sie unter Löschen oder Deaktivieren von Metrikalarmen.
- Fügen Sie Ihre E-Mail-Adresse und Mobiltelefonnummer als Benachrichtigungskontakte in Lightsail hinzu, um wieder E-Mail- und SMS-Benachrichtigungen zu erhalten. Weitere Informationen finden Sie unter Hinzufügen von Benachrichtigungskontakten.

Tags in Amazon Lightsail

Amazon Lightsail ermöglicht es Ihnen, Ihren Ressourcen Bezeichnungen als Tags zuzuweisen. Jedes Tag ist ein Label, das aus einem Schlüssel und einem optionalen Wert besteht, der die Verwaltung, Suche und Filterung von Ressourcen effizienter gestalten kann.

Amazon Lightsail ermöglicht es Ihnen, Ihren Ressourcen Bezeichnungen als Tags zuzuweisen. Jedes Tag ist ein Label, das aus einem Schlüssel und einem optionalen Wert besteht, der die Verwaltung, Suche und Filterung von Ressourcen effizient gestalten kann. Obwohl es keine inhärenten Typen von Tags gibt, können Sie Lightsail-Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien kategorisieren. Dies ist nützlich, wenn Sie viele Ressourcen desselben Typs haben. Sie können eine bestimmte Ressource anhand der ihr zugewiesenen Tags schnell identifizieren. Definieren Sie beispielsweise einen Satz von Tags für Ihre Ressourcen, mit denen Sie das Projekt oder die Priorität jeder Ressource verfolgen können.

Ein Schlüssel ohne Wert wird in Lightsail als Key-only-Tag (Nur-Schlüssel-Tag) bezeichnet. Ein Schlüssel mit einem Wert wird als Key-Value-Tag (Schlüssel-Wert-Tag) bezeichnet. Das folgende Diagramm veranschaulicht, wie Markieren funktioniert. In diesem Beispiel verfügt jede Ressource über einen Satz von Schlüssel-Wert-Tag und Nur-Schlüssel-Tag. Die Schlüssel-Wert-Tags identifizieren Projekte und Prioritäten und Nur-Schlüssel-Tags identifizieren Kunden und Anwendungsversionen.



Organisieren der Verrechnung und Steuern des Zugriffs mit Tags

Sie können Tags auch verwenden, um Ihre Abrechnung zu organisieren, den Zugriff auf Ressourcen und Anfragen in Lightsail zu steuern und den Zugriff auf die Tag-Schlüssel zu kontrollieren. Weitere Informationen finden Sie in einem der folgenden Handbücher:

- Verwenden von Tags zur Organisation der Ressourcenkosten
- Verwendung von Tags zur Kontrolle des Ressourcenzugriffs

Lightsail-Ressourcen, die das Tagging unterstützen

Sie können die meisten Lightsail-Ressourcen mit Tags markieren, wenn Sie sie erstellen oder nachdem sie erstellt wurden. Wenn Tags während der Ressourcenerstellung nicht angewendet werden können, setzt Lightsail den Prozess der Ressourcenerstellung zurück. Auf diese Weise wird sichergestellt, dass Ressourcen entweder mit Tags erstellt oder gar nicht erstellt werden, und dass keine Ressourcen, die markiert werden sollten, immer unmarkiert bleiben.

Die folgenden Lightsail-Ressourcen können in der Lightsail-Konsole markiert werden:

- Instances
- Containerdienste
- Netzwerkverteilungen zur Bereitstellung von Inhalten (CDN)
- Buckets
- Datenbanken
- Laufwerke
- DNS-Zonen
- Load Balancers

> **Important**
>
> Snapshots, die mit der Lightsail-Konsole erstellt wurden, erben automatisch Tags von der Quellressource. Eine Lightsail-Ressource, die aus einem Snapshot erstellt wurde, weist die gleichen Tags auf, die auch auf der Quellressource vorhanden waren, als der Snapshot erstellt wurde.

Die folgenden Ressourcen können mithilfe der Lightsail-API, AWS Command Line Interface (AWS CLI) oder SDKs markiert werden:

- Datenbank-Snapshots
- Datenbanken

- Datenträger-Snapshots
- Laufwerke
- Domänen (DNS-Zonen)
- Instance-Snapshots
- Instances
- Schlüsselpaare
- Load Balancer TLS-Zertifikate (TLS-Zertifikate, die mit Lightsail erstellt wurden)
- Load Balancers

> **Important**
>
> Snapshots, die mit der Lightsail-API, AWS CLI oder SDKs erstellt wurden, erben nicht automatisch Tags von der Quellressource. Stattdessen müssen Sie die Tags der Quellressource manuell mit dem `tags`-Parameter angeben.

Tag (Markierung)-Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags (Markierungen):

- Maximale Anzahl von Tags pro Ressource – 50.
- Für jede Ressource muss jeder Tag-Schlüssel eindeutig sein. Jeder Tag-Schlüssel kann nur einen Wert haben.
- Maximale Schlüssellänge – 128 Unicode-Zeichen in UTF-8.
- Maximale Wertlänge – 256 Unicode-Zeichen in UTF-8.
- Wenn Ihr Markierungsschema für mehrere -Services und -Ressourcen verwendet wird, denken Sie daran, dass andere Services möglicherweise Einschränkungen für zulässige Zeichen haben. Allgemein erlaubte Zeichen sind: Buchstaben, Zahlen und Leerzeichen, und die folgenden Sonderzeichen: + - = . _ : / @
- Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden.
- Verwenden Sie nicht das `aws:`-Präfix für Schlüssel oder Werte. Dieses Präfix ist für die Verwendung in AWS reserviert.

Lightsail-Ressourcen-Tags hinzufügen

Verwenden Sie Tags in Amazon Lightsail, um Ihre Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Tags können den Ressourcen bei oder nach der Erstellung hinzugefügt werden. Führen Sie diese Schritte aus, um einer Ressource nach ihrer Erstellung Tags hinzuzufügen.

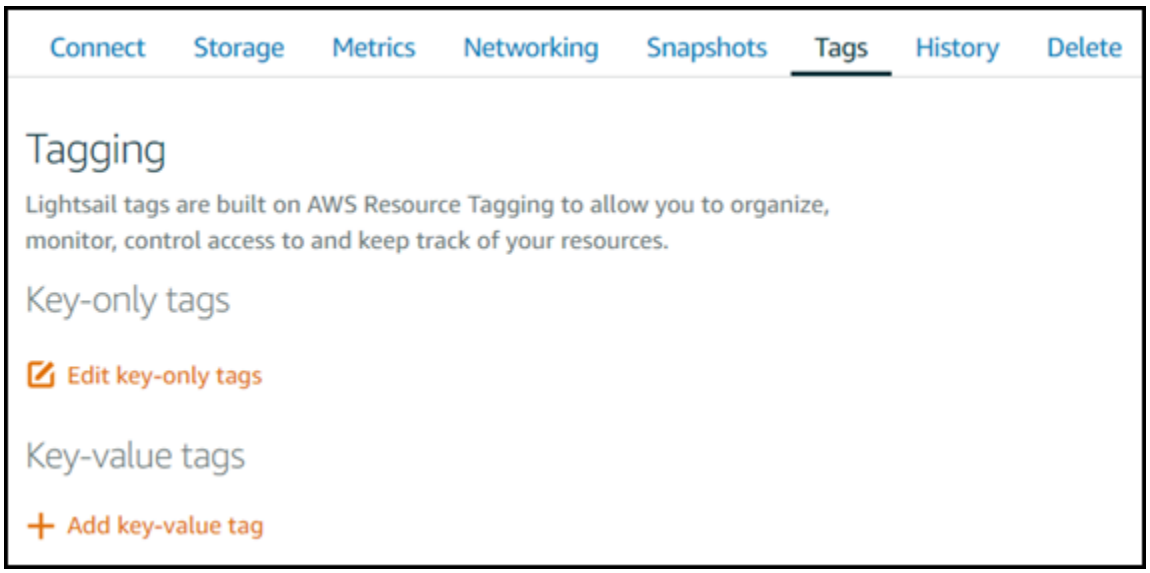
> **Note**
>
> Weitere Informationen über Tags, welche Ressourcen markiert werden können und welche Einschränkungen es gibt, finden Sie unter Tags.

So fügen Sie einer Ressource Tags hinzu

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte für den Ressourcentyp aus, den Sie markieren möchten. Um beispielsweise ein Tag zu einer DNS-Zone hinzuzufügen, wählen Sie die Registerkarte Networking (Netzwerk) aus. Oder wählen Sie die Registerkarte Instances aus, um einer Instance ein Tag hinzuzufügen.

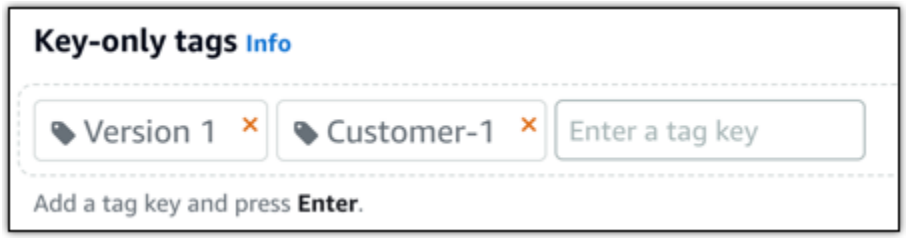
   > **Note**
   >
   > Instances, Containerdienste, CDN-Verteilungen, Buckets, Datenbanken, Datenträger, DNS-Zonen und Load Balancers können mit der Lightsail-Konsole markiert werden. Weitere Lightsail-Ressourcen können zusätzlich mit Lightsail-API-Operationen, der AWS Command Line Interface (AWS CLI) oder SDKs markiert werden. Eine vollständige Liste der Lightsail-Ressourcen, die das Markieren unterstützen, finden Sie unter Tags.

3. Wählen Sie die Ressource aus, die Sie markieren möchten.
4. Wählen Sie auf der Verwaltungsseite für die von Ihnen ausgewählte Ressource die Registerkarte Tags aus.



5. Wählen Sie eine der folgenden Optionen aus, je nachdem, welche Art von Tag Sie hinzufügen möchten:

   - Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.

   - Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

     Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.

Nächste Schritte

Weitere Informationen zu Aufgaben, die Sie nach dem Hinzufügen von Tags zu einer Ressource ausführen können, finden Sie in den folgenden Anleitungen:

- Verwendung von Tags, um Ihre Ressourcen zu organisieren
- Verwendung von Tags zur Organisation der Kosten für Ihre Ressourcen
- Verwendung von Tags zur Steuerung des Zugriffs auf Ihre Ressourcen
- Löschen von Tags

Löschen von Tags in Lightsail

Sie können Tags von einer Amazon Lightsail-Ressource löschen. Das Löschen eines Tags von einer Ressource löscht das Tag nicht von allen anderen Ressourcen. Um ein Tag vollständig von allen Ressourcen zu löschen, müssen Sie dieses Tag von jeder Ressource entfernen. In diesem Handbuch werden die Schritte zum Löschen von Tags von einer Ressource beschrieben.

> **Note**
>
> Weitere Informationen über Tags, welche Ressourcen markiert werden können und welche Tag-Einschränkungen es gibt, finden Sie unter Tags.

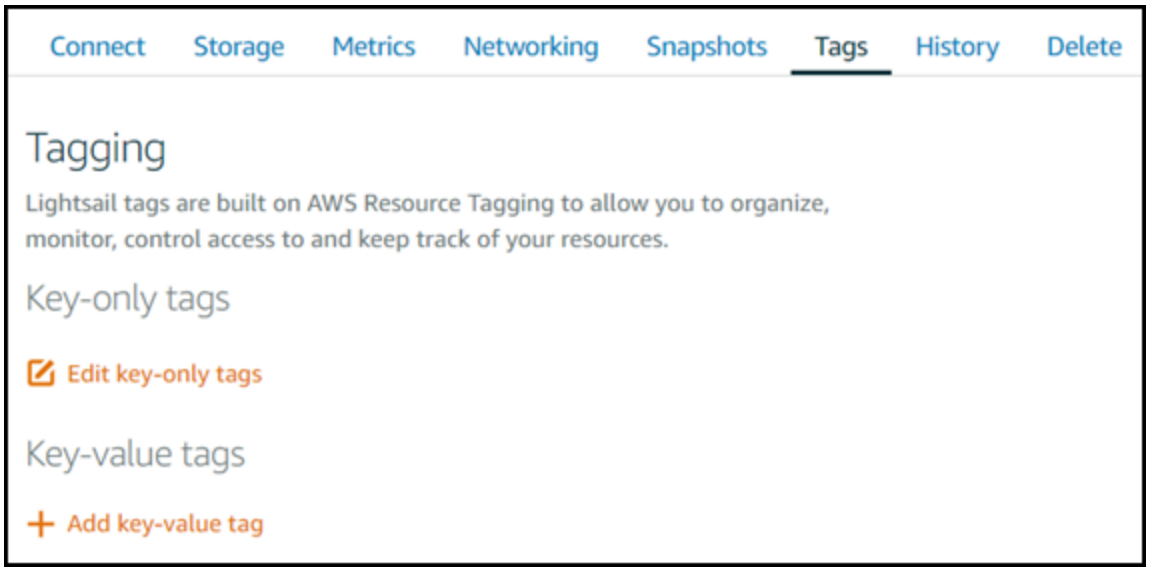
So löschen Sie Tags von einer Ressource

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte für den Ressourcentyp aus, von dem Sie Tags löschen möchten. Um beispielsweise Tags von einer DNS-Zone zu löschen, wählen Sie

die Registerkarte Networking (Netzwerk) aus. Oder wählen Sie die Registerkarte Instances aus, um Tags von einer Instance zu löschen.

> **Note**
>
> Instances, Containerdienste, CDN-Verteilungen, Buckets, Datenbanken, Datenträger, DNS-Zonen und Load Balancern können mit der Lightsail-Konsole markiert werden. Weitere Lightsail-Ressourcen können zusätzlich mit Lightsail-API-Operationen, der AWS-Befehlszeilenschnittstelle (AWS CLI) oder SDKs markiert werden. Eine vollständige Liste der Lightsail-Ressourcen, die das Markieren unterstützen, finden Sie unter Tags.

3. Wählen Sie die Ressource aus, von der Sie die Tags löschen möchten.
4. Wählen Sie auf der Verwaltungsseite für die von Ihnen ausgewählte Ressource die Registerkarte Tags aus.



5. Führen Sie je nach Art des Tags, das Sie aus der Ressource löschen möchten, einen der folgenden Schritte aus:

   a. Wählen Sie Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) aus und wählen Sie dann das Löschsymbol (X) für den Tag aus, den Sie von der Ressource löschen möchten. Wählen Sie Save (Speichern) aus, wenn Sie keine Tags mehr löschen möchten, um sie von der Ressource zu entfernen, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht zu entfernen.

b. Um ein Schlüssel-Wert-Tag zu entfernen, wählen Sie das Löschsymbol (X) für das Schlüssel-Wert-Tag aus. Wählen Sie bei Aufforderung Yes, delete (Ja, löschen) aus, um den Schlüssel-Wert-Tag zu entfernen, oder wählen Sie No, cancel (Nein, abbrechen) aus, um ihn nicht zu entfernen.

Unterstützung für Berechtigungen auf Ressourcenebene und Autorisierung auf der Basis von Tags in Lightsail

Lightsail unterstützt teilweise Berechtigungen auf Ressourcenebene und Autorisierung auf der Basis von Tags, für manche ihrer API-Aktionen. Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lightsail in der Service-Autorisierungs-Referenz.

Verwendung von Tags zur Kontrolle des Lightsail-Ressourcenzugriffs

Sie können Tags in Amazon Lightsail verwenden, um den Zugriff auf Ressourcen, den Zugriff auf Anfragen und den Zugriff auf Tag-Schlüssel zu steuern. In diesem Handbuch erfahren Sie, wie Sie eine AWS Identity and Access Management (IAM)-Richtlinie erstellen, die ein Schlüssel-Wert-Tag festlegt, das zum Erstellen oder Löschen von Lightsail-Ressourcen erforderlich ist, und die Richtlinie an Benutzer oder Gruppen für diese Anforderungen anhängen.

> **Note**
>
> Um mehr über Tags in Lightsail, die markierbaren Ressourcen und die Einschränkungen zu erfahren, lesen Sie Tags.

Schritt 1: Erstellen einer IAM-Richtlinie

Erstellen Sie zunächst die folgenden IAM-Richtlinien in der IAM-Konsole. Informationen zum Erstellen einer IAM-Richtlinie finden Sie unter Erstellen von IAM-Richtlinien in der IAM-Dokumentation.

Die folgende Richtlinie beschränkt die Erstellung neuer Lightsail-Ressourcen durch Benutzer – es sei denn, mit der Erstellungsanforderung wird der Schlüssel `allow` und der Wert `true` definiert. Diese Richtlinie beschränkt außerdem das Löschen von Ressourcen, es sei denn, sie haben den Schlüssel-Wert-Tag `allow/true`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:Create*",
                "lightsail:TagResource",
                "lightsail:UntagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/allow": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:Delete*",
                "lightsail:TagResource",
                "lightsail:UntagResource"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/allow": "true"
                }
            }
        }
    ]
}
```

Die folgende Richtlinie hindert Benutzer daran, den Tag für Ressourcen zu ändern, die einen anderen Schlüssel-Wert-Tag als `allow/false` haben.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "lightsail:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:ResourceTag/allow": "false"
                }
            }
        }
    ]
}
```

Schritt 2: Anhängen der Richtlinie an Benutzer oder Gruppen

Nachdem Sie die IAM-Richtlinien erstellt haben, fügen Sie sie den Benutzern oder Gruppen hinzu, die Lightsail-Ressourcen mithilfe des Schlüssel-Werte-Paares erstellen müssen. Weitere Informationen zum Anhängen von IAM-Richtlinien an Benutzer oder Gruppen finden Sie unter Hinzufügen und Entfernen von IAM-Richtlinien in der IAM-Dokumentation.

Verwenden Sie Tags zum Organisieren der Lightsail-Ressourcenkosten

Sie können Tags in Amazon Lightsail verwenden, um Ihre AWS-Abrechnung so zu organisieren, dass sie Ihrer eigenen Kostenstruktur entspricht. Dazu fügen Sie Ihren Lightsail-Ressourcen Schlüssel-Wert-Tags hinzu. Dann aktivieren Sie diese Tags in der AWS Billing and Cost Management-Konsole. Melden Sie sich abschließend an, um Ihre AWS-Kontorechnung mit den Schlüssel-Wert-Tags in Ihrem Kostenzuordnungsbericht zu erhalten. Diese Anleitung enthält die Schritte für die Einrichtung.

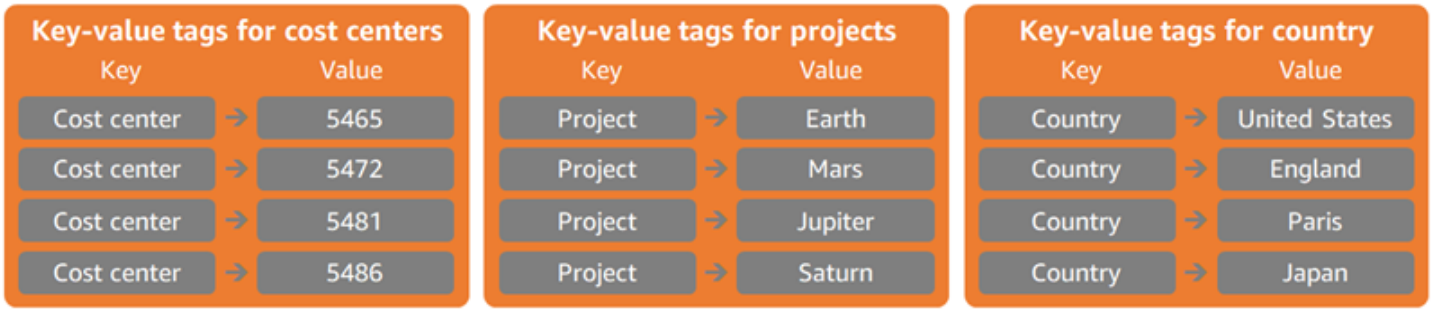
> **Note**
>
> Weitere Informationen über Tags in Lightsail, welche Ressourcen markiert werden können und welche Tag-Einschränkungen es gibt, finden Sie unter Tags.

> **Important**
>
> Lightsail-Datenbank-Snapshots können derzeit im Kostenzuordnungsbericht nicht verfolgt werden, auch wenn ihnen ein Kostenzuordnungs-Tag hinzugefügt wurde.

Schritt 1: Fügen Sie Schlüssel-Wert-Tags zu den -Ressourcen hinzu

Fügen Sie Schlüssel-Wert-Tags zu den Lightsail-Ressourcen hinzu, die Sie in Ihrer Fakturierungskonsole organisieren möchten. Weitere Informationen über Schlüssel-Wert-Tags finden Sie unter Hinzufügen von Tags zu einer Ressource.

Sie können einen Satz von Tag-Schlüsseln entwickeln, die widerspiegeln, wie Sie Ihre Kosten organisieren wollen. Ihr Kostenzuordnungsbericht zeigt die Tag-Schlüssel als zusätzliche Spalten mit den entsprechenden Werten für jede Zeile an. Es ist jedenfalls effizienter, Ihre Kosten mit einem einheitlichen Satz von Tag-Schlüssel zu verfolgen. So können Sie beispielsweise mehrere Lightsail-Ressourcen mit einer bestimmten Kostenstelle markieren. Hierzu verwenden Sie einen "Kostenstellen-Schlüssel" in Verbindung mit einem Zahlenwert. Organisieren Sie Ihre Abrechnungsinformationen dann so, dass Sie die Abrechnung für diese Kostenstelle über mehrere Ressourcen hinweg sehen können. Das folgende Beispiel zeigt Schlüssel-Wert-Tags, die zur Organisation der Kostenzuordnung verwendet werden können:



Schritt 2: Aktivieren Sie die benutzerdefinierten Kostenzuordnungs-Tags

Nachdem Sie Ihren Lightsail-Ressourcen die erforderlichen Tags hinzugefügt haben, aktivieren Sie diese für die Kostenzuordnung in der Konsole für Rechnungs- und Kostenverwaltung. Wenn Sie beispielsweise einen Schlüssel-Tag „Kostenstelle“ erstellt haben, aktivieren Sie diesen Schlüssel-Tag in der Konsole für Rechnungs- und Kostenverwaltung, um Kostenzuordnungsberichte für diesen Schlüssel-Tag zu erstellen. Weitere Informationen finden Sie unter Benutzerdefinierte Kostenzuordnungs-Tags aktivieren in der AWS Billing and Cost Management-Dokumentation.

Schritt 3: Legen Sie den Kostenzuordnungsbericht fest und zeigen Sie ihn an

Der monatliche Kostenzuordnungsbericht listet die AWS-Nutzung für Ihr Konto nach Produktkategorie und verbundenem Benutzer auf. Der Bericht enthält die gleichen Einzelposten wie Ihr detaillierter Abrechnungsbericht und zusätzliche Spalten für Ihre Tag-Schlüssel. Weitere Informationen zum Einrichten des monatlichen Kostenzuordnungsberichts finden Sie unter Einrichten des monatlichen Kostenzuordnungsberichts in der AWS Billing and Cost Management-Dokumentation.

Wenn Sie den Kostenzuordnungsbericht einrichten, haben Sie ein Amazon Simple Storage Service (Amazon S3)-Bucket definiert, in dem der Bericht gespeichert wird. Öffnen Sie den von Ihnen definierten Amazon-S3-Bucket und öffnen Sie den Kostenzuordnungsbericht, sobald er verfügbar ist. Weitere Informationen über die Inhalte des Kostenzuordnungsberichts finden Sie unter Anzeigen eines Kostenzuordnungsberichts in der AWS Billing and Cost Management-Dokumentation.

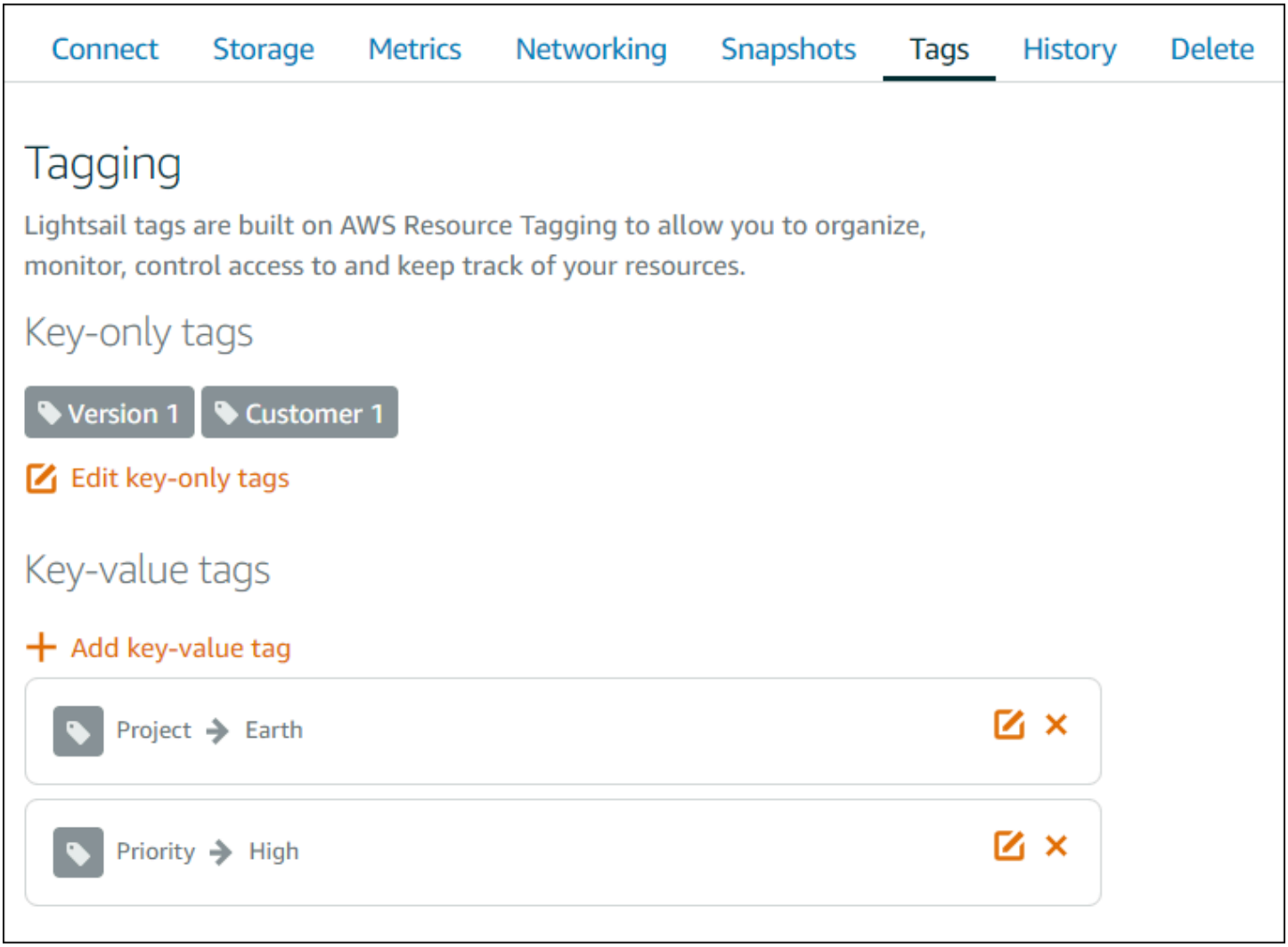
Tags verwenden, um Ihre Lightsail-Ressourcen zu organisieren

Nachdem Sie Ihre Amazon Lightsail-Ressourcen markiert haben, können Sie Ihre Ressourcen mit den von Ihnen hinzugefügten Tags filtern. Verwenden Sie dazu die Lightsail-Konsole und wählen oder suchen Sie einen Tag. Dieser Leitfaden zeigt Ihnen, wie Sie Ihre Lightsail-Ressourcen nach Tags anzeigen und filtern können.

> **Note**
>
> Weitere Informationen über Tags, welche Ressourcen markiert werden können und welche Tag-Einschränkungen es gibt, finden Sie unter Tags.

Anzeigen von Tags für eine Ressource

Instances, Containerdienste, CDN-Verteilungen, Buckets, Datenbanken, Datenträger, DNS-Zonen und Load Balancers können mit der Lightsail-Konsole markiert werden und enthalten daher eine Registerkarte Tags. Diese Registerkarte ist über die Verwaltungsseite der Ressource zugänglich, wie im folgenden Beispiel für eine Instance-Ressource gezeigt. Sie können die Registerkarte Tags zum Hinzufügen, Löschen oder Bearbeiten von Tags verwenden. Weitere Informationen finden Sie unter Hinzufügen von Tags zu einer Ressource und Löschen von Tags.



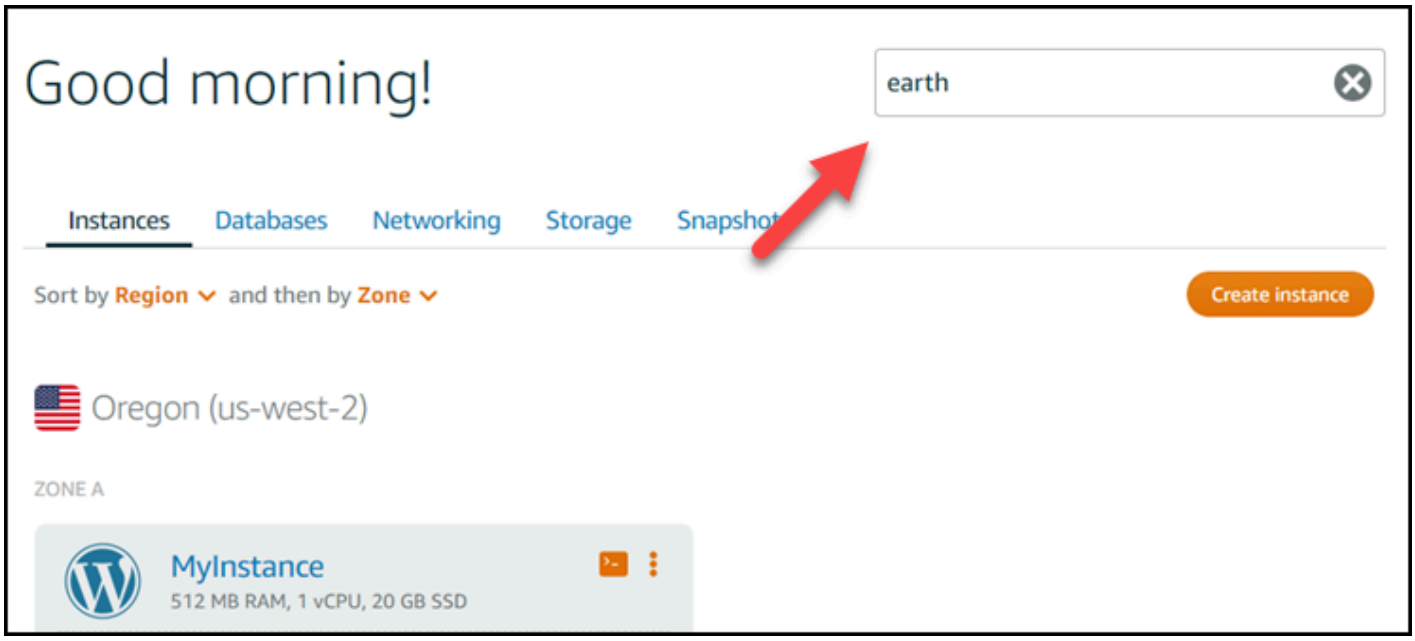
> **Note**
>
> Instances, Containerdienste, CDN-Verteilungen, Buckets, Datenbanken, Datenträger, DNS-Zonen und Load Balancers können mit der Lightsail-Konsole markiert werden. Weitere Lightsail-Ressourcen können zusätzlich mit Lightsail-API-Operationen, der AWS Command Line Interface (AWS CLI) oder SDKs markiert werden. Eine vollständige Liste der Lightsail-Ressourcen, die das Markieren unterstützen, finden Sie unter Tags.

Filtern von Ressourcen mit Tags

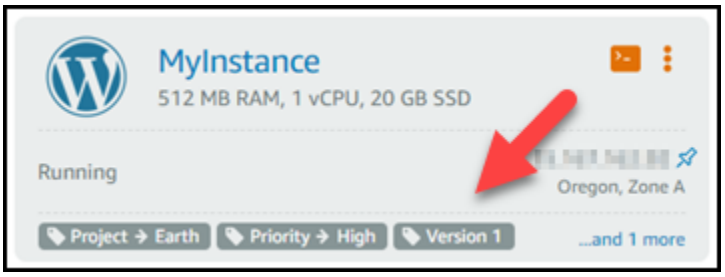
Die folgenden Optionen sind in der Lightsail-Konsole verfügbar, um Ihre Ressourcen mit Tags filtern. Alle diese Optionen aktualisieren die Lightsail-Startseite, damit sie nur den Tag anzeigt, den Sie gesucht oder ausgewählt haben.

> **Note**
>
> Diese Filteroptionen sind dauerhaft. Wenn Sie nach einem Tag filtern und dann zwischen den Abschnitten der Lightsail-Startseite navigieren, wird der Filter weiterhin angewendet.

- Geben Sie auf der Lightsail-Startseite den Nur-Schlüssel-Tag oder den Wert in das Textfeld Search (Suchen) ein, nachdem Sie filtern möchten, und drücken Sie auf Enter (Eingabetaste).



- Wählen Sie einen Tag, der unter einer Ressource auf der Lightsail-Startseite angezeigt wird.



- Wählen Sie einen Tag, der in der Überschrift einer Ressource angezeigt wird.

Problembehebung bei Amazon Lightsail-Ressourcen

Die folgenden Themen können Ihnen bei der Behebung von Problemen helfen, die möglicherweise mit Ihren Amazon Lightsail-Ressourcen auftreten.

Themen

Fehlerbehebung bei der WordPress Einrichtung in Lightsail

Während des WordPress Einrichtungs-Workflows in Amazon Lightsail können zwei Arten von Fehlermeldungen auftreten:

Häufige Fehler

Diese Arten von Fehlern treten sofort auf, nachdem Sie im letzten Schritt des Workflows die Option Zertifikat erstellen ausgewählt haben. Diese Fehler werden in einem Banner oben in der Lightsail-Konsole angezeigt. Sie werden in der Regel dadurch verursacht, dass der Setup-Workflow auf älteren WordPress Instanzen ausgeführt wird oder dass falsche Informationen übermittelt werden. Wählen Sie beispielsweise einen DNS-Eintrag aus, der nicht auf die öffentliche IP-Adresse Ihrer Instance verweist.

Fehler bei der Einrichtung

Diese Art von Fehlern tritt innerhalb weniger Minuten auf, nachdem Sie den letzten Schritt im Workflow abgeschlossen haben. Diese Fehlermeldungen werden im Bereich WordPress Website

einrichten auf dem Tab Instance Connect angezeigt. Diese Fehler treten auf, wenn das Let's Encrypt HTTPS-Zertifikat auf Ihrer Instance nicht konfiguriert werden kann.

Verwenden Sie die Informationen in den folgenden Themen, um Fehler zu diagnostizieren und zu beheben, die beim WordPress Setup Guided Workflow auftreten könnten.

Themen

- Behebung häufiger WordPress Einrichtungsfehler in Lightsail
- Behebung von WordPress Einrichtungsfehlern in Lightsail

Weitere Informationen zum WordPress einrichtungsgesteuerten Workflow in Amazon Lightsail finden Sie unter Konfiguration Ihrer WordPress Instance.

Behebung häufiger WordPress Einrichtungsfehler in Lightsail

Wenn es ein Problem mit den während des Workflows übermittelten Informationen gibt, wird oben in der Lightsail-Konsole eine Fehlermeldung angezeigt.

In der ersten Zeile der Meldung werden Sie darüber informiert, dass beim Setup ein Fehler aufgetreten ist:

Das Setup auf Ihrer Instance *InstanceName*in der *InstanceRegion*Region konnte nicht abgeschlossen werden.

Die zweite Zeile enthält den Fehler, auf den das Setup gestoßen ist:

Es ist ein Fehler aufgetreten und wir konnten keine Verbindung zu Ihrer Instance herstellen oder die Verbindung zu Ihrer Instance aufrechterhalten

Um mit der Problembehandlung zu beginnen, ordnen Sie den in der Meldung angezeigten Fehler einem der folgenden Fehler zu.

Fehler

- DNS-Einträge wurden nicht gefunden. Vergewissern Sie sich, dass die DNS-Einträge der Domain auf die öffentliche IP-Adresse Ihrer Instance verweisen, und warten Sie, bis die DNS-Änderungen wirksam werden.

- Die DNS-Einträge stimmen nicht überein. Vergewissern Sie sich, dass die DNS-Einträge der Domain auf die öffentliche IP-Adresse Ihrer Instance verweisen, und warten Sie, bis die DNS-Änderungen wirksam werden.
- Es konnte keine Verbindung zu Ihrer Instance hergestellt werden. Warten Sie einige Minuten, bis die SSH-Verbindung bereit ist. Starten Sie dann die Einrichtung erneut.
- Nicht unterstützte Version. WordPress Setup unterstützt nur WordPress Versionen 6 und höher.
- Setup unterstützt nur WordPress Instanzen, die am oder nach dem 1. Januar 2023 erstellt wurden.
- Die Firewall-Ports 22, 80 und 443 der Instanz müssen während des Einrichtungs-Workflows eine TCP-Verbindung von einer beliebigen IP-Adresse aus zulassen. Sie können diese Einstellungen auf der Registerkarte Instanznetzwerk ändern.

DNS-Einträge wurden nicht gefunden. Vergewissern Sie sich, dass die DNS-Einträge der Domain auf die öffentliche IP-Adresse Ihrer Instance verweisen, und warten Sie, bis die DNS-Änderungen wirksam werden.

Grund

Dieser Fehler wird durch falsch konfigurierte DNS-Einträge oder DNS-Einträge verursacht, die nicht genügend Zeit hatten, um sich im DNS des Internets zu verbreiten.

Korrigieren

Vergewissern Sie sich, dass die A - oder AAAA-DNS-Einträge in der DNS-Zone vorhanden sind und dass sie auf die öffentliche IP-Adresse Ihrer Instance verweisen. Weitere Informationen finden Sie unter DNS in Lightsail.

Wenn Sie DNS-Einträge hinzufügen oder aktualisieren, die auf Traffic von Ihrer Apex-Domain (`example.com`) und deren `www` Subdomänen (`www.example.com`) verweisen, müssen sie sich über das DNS des Internets verbreiten. Mithilfe von Tools wie nslookup oder DNS Lookup von können Sie überprüfen, ob Ihre DNS-Änderungen wirksam wurden. MxToolbox

> **Note**
>
> Warten Sie, bis sich Änderungen an DNS-Einträgen über das DNS des Internets verbreitet haben. Dies kann mehrere Stunden dauern.

Die DNS-Einträge stimmen nicht überein. Vergewissern Sie sich, dass die DNS-Einträge der Domain auf die öffentliche IP-Adresse Ihrer Instance verweisen, und warten Sie, bis die DNS-Änderungen wirksam werden.

Grund

Die A - oder AAAA-DNS-Einträge verweisen nicht auf die öffentliche IP-Adresse der Instance.

Korrigieren

Vergewissern Sie sich, dass die A - oder AAAA-DNS-Einträge in der DNS-Zone vorhanden sind und dass sie auf die öffentliche IP-Adresse Ihrer Instance verweisen. Weitere Informationen finden Sie unter DNS in Lightsail.

> **Note**
>
> Warten Sie, bis sich Änderungen an DNS-Einträgen über das DNS des Internets übertragen haben. Dies kann mehrere Stunden dauern.

Es konnte keine Verbindung zu Ihrer Instance hergestellt werden. Warten Sie einige Minuten, bis die SSH-Verbindung bereit ist. Starten Sie dann die Einrichtung erneut.

Grund

Die Instanz wurde gerade erstellt oder neu gestartet und die SSH-Verbindung ist nicht bereit.

Reparieren

Warten Sie einige Minuten, bis die SSH-Verbindung bereit ist. Versuchen Sie dann erneut, den geführten Workflow auszuführen. Weitere Informationen finden Sie unter SSH-Fehlerbehebung in Lightsail.

Nicht unterstützte Version. WordPress Setup unterstützt nur WordPress Versionen 6 und höher.

Grund

Die Version WordPress , die auf der Instanz installiert ist, ist älter als WordPress Version 6. Ältere WordPress Versionen enthalten inkompatible Software und Abhängigkeiten, die verhindern, dass das HTTPS-Zertifikat generiert wird.

Korrigieren

Erstellen Sie eine neue WordPress Instanz von der Lightsail-Konsole aus. Migrieren Sie dann die WordPress Website von der älteren auf die neue Instanz. Weitere Informationen finden Sie unter Migrieren eines vorhandenen WordPress Blogs.

Wenn Sie eine neue Instanz erstellen, um die bestehende Instanz zu ersetzen, stellen Sie sicher, dass Sie Ihre Anwendungsabhängigkeiten auf Ihre neue Instanz aktualisieren.

Setup unterstützt nur WordPress Instanzen, die am oder nach dem 1. Januar 2023 erstellt wurden.

Grund

Die Instanz, die mit dem Setup verwendet wird, enthält möglicherweise veraltete Software. Ältere Software verhindert die Generierung des HTTPS-Zertifikats.

Korrigieren

Erstellen Sie eine neue WordPress Instanz von der Lightsail-Konsole aus. Migrieren Sie dann die WordPress Website von der älteren auf die neue Instanz. Weitere Informationen finden Sie unter Migrieren eines vorhandenen WordPress Blogs.

Wenn Sie eine neue Instanz erstellen, um die bestehende Instanz zu ersetzen, stellen Sie sicher, dass Sie Ihre Anwendungsabhängigkeiten auf Ihre neue Instanz aktualisieren.

Die Firewall-Ports 22, 80 und 443 der Instanz müssen während des Einrichtungs-Workflows eine TCP-Verbindung von einer beliebigen IP-Adresse aus zulassen. Sie können diese Einstellungen auf der Registerkarte Instanznetzwerk ändern.

Grund

Die Firewall-Ports 22, 80 und 443 der Instanz müssen TCP-Verbindungen von jeder IP-Adresse aus zulassen, während das Setup ausgeführt wird. Dieser Fehler wird generiert, wenn einer oder mehrere dieser Ports geschlossen werden. Weitere Informationen finden Sie unter Instance-Firewalls.

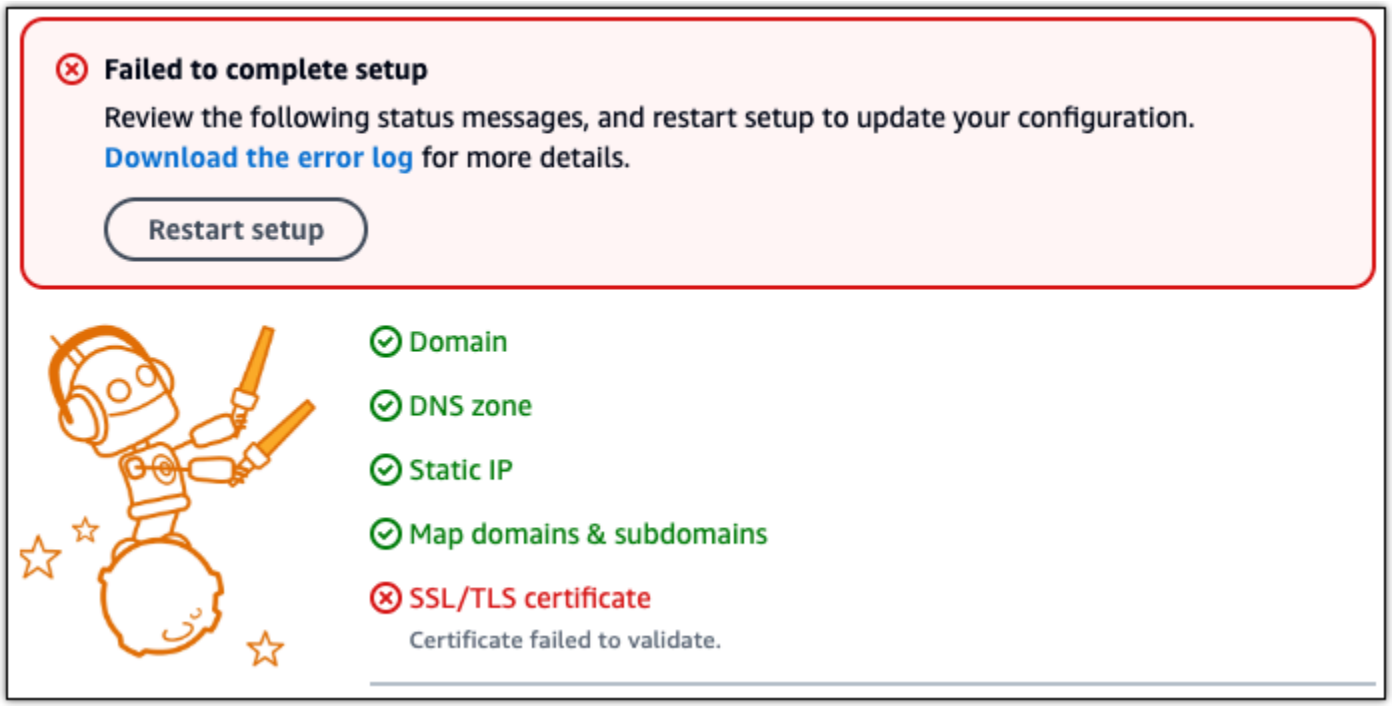
Korrigieren

Fügen Sie die IPv4- und IPv6-Firewallregeln der Instanz hinzu oder bearbeiten Sie sie, um TCP-Verbindungen über die Ports 22, 80 und 443 zuzulassen. Weitere Informationen finden Sie unter Firewallregeln für Instanzen hinzufügen und bearbeiten.

Behebung von WordPress Einrichtungsfehlern in Lightsail

Fehlermeldungen bei der Installation werden im Bereich WordPressWebsite einrichten auf dem Tab Instance Connect angezeigt. Fehler bei der Einrichtung können innerhalb weniger Minuten auftreten, nachdem Sie den letzten Schritt im Workflow abgeschlossen haben. Sie werden verursacht, wenn das Let's Encrypt HTTPS-Zertifikat auf Ihrer Instanz nicht konfiguriert werden kann.

Setup konnte nicht abgeschlossen werden — Überprüfen Sie die folgenden Statusmeldungen und starten Sie das Setup neu, um Ihre Konfiguration zu aktualisieren. Laden Sie das Fehlerprotokoll für weitere Informationen herunter.



Wählen Sie in der Fehlermeldung den Link Fehlerprotokoll herunterladen, um die vom Setup generierten Fehlerprotokolle herunterzuladen und anzuzeigen. Um mit der Problembehandlung zu beginnen, ordnen Sie die Fehlermeldung aus den Protokollen einem der folgenden Fehler zu.

Fehler

- CertBot. Fehler. AuthorizationError: Einige Herausforderungen sind gescheitert
- Certbot konnte einige Domänen nicht authentifizieren
- In den letzten 168 Stunden wurden bereits zu viele Zertifikate (5) für genau diese Gruppe von Domains ausgestellt
- Zu viele fehlgeschlagene Autorisierungen

CertBot. Fehler. AuthorizationError: Einige Herausforderungen sind gescheitert

Grund

Dieser Fehler wird durch falsch konfigurierte DNS-Einträge oder DNS-Einträge verursacht, die nicht genügend Zeit hatten, um sich im Internet zu verbreiten.

Korrigieren

Stellen Sie sicher, dass die A - oder AAAA-DNS-Einträge in der DNS-Zone vorhanden sind und dass sie auf die öffentliche IP-Adresse Ihrer Instance verweisen. Weitere Informationen finden Sie unter DNS in Lightsail.

Wenn Sie DNS-Einträge hinzufügen oder aktualisieren, die auf Traffic von Ihrer Apex-Domäne (`example.com`) und deren `www` Subdomänen (`www.example.com`) verweisen, müssen sie sich über das Internet verbreiten. Sie können überprüfen, ob Ihre DNS-Änderungen wirksam wurden, indem Sie Tools wie nslookup oder DNS Lookup from verwenden. MxToolbox

> **Note**
>
> Warten Sie, bis sich Änderungen an DNS-Einträgen über das DNS des Internets verbreitet haben. Dies kann mehrere Stunden dauern.

Certbot konnte einige Domänen nicht authentifizieren

Grund

Dieser Fehler kann auftreten, wenn ein anderer Prozess Port 80 verwendet, während das HTTPS-Zertifikat auf der Instanz konfiguriert wird.

Korrigieren

Starten Sie Ihre WordPress Instanz neu. Führen Sie dann den geführten Workflow erneut aus. Gehen Sie wie folgt vor, um alle laufenden Prozesse auf der Instance zu beenden, die auf Port 80 ausgeführt werden, falls das Problem durch einen Neustart nicht behoben wird.

Verfahren

1. Connect zu Ihrer Instance her, indem Sie den browserbasierten Lightsail-SSH-Client verwenden, oder indem Sie AWS CloudShell
2. Stoppen Sie den Bitnami-Prozess, der auf der Instanz ausgeführt wird:

```
$ sudo /opt/bitnami/ctlscript.sh stop
```

Stellen Sie sicher, dass der Bitnami-Prozess gestoppt wurde:

```
sudo /opt/bitnami/ctlscript.sh status
```

3. Prüfen Sie, ob es andere Prozesse gibt, die Port 80 verwenden:

```
fuser -n tcp 80
```

4. Beenden Sie alle Prozesse, die nicht von einer anderen Anwendung benötigt werden:

```
fuser -k -n tcp 80
```

5. Starten Sie das WordPress Setup neu.

In den letzten 168 Stunden wurden bereits zu viele Zertifikate (5) für genau diese Gruppe von Domains ausgestellt

Grund

Eine oder mehrere Ihrer Domains oder Subdomains wurden innerhalb der letzten Woche bereits zur Erstellung von 5 Zertifikaten verwendet. Weitere Informationen finden Sie unter Ratenlimits auf der Let's Encrypt-Website.

Korrigieren

Warten Sie eine Woche (168 Stunden), und starten Sie dann den geführten Workflow für diese Domain neu.

Zu viele fehlgeschlagene Autorisierungen

Grund

Eine oder mehrere der Domains oder Subdomains in der Anfrage haben das Limit von fünf Validierungen pro Stunde überschritten. Weitere Informationen finden Sie unter Ratenlimits auf der Let's Encrypt-Website.

Korrigieren

Warten Sie eine Stunde und führen Sie das WordPress Setup erneut aus. Vergewissern Sie sich, dass andere Überprüfungsfehler behoben wurden, bevor Sie das Setup neu starten.

Beheben Sie einen 403-Fehler (nicht autorisiert) in Lightsail

Wenn Sie beim Versuch, auf die Lightsail-Konsole zuzugreifen, einen Fehler 403 erhalten, geraten Sie nicht in Panik. Probieren Sie die folgenden Schritte aus, um das Problem zu beheben:

- Wenn Ihr AWS-Konto oder Ihr AWS Identity and Access Management (IAM)-Benutzer vor Kurzem erstellt wurde, warten Sie einige Minuten und aktualisieren Sie den Browser.
- Wenn es schon eine Weile her ist, dass Sie sich zuletzt angemeldet haben, aktualisieren Sie Ihren Browser. Wenn Sie aufgefordert werden, sich erneut anzumelden, stellen Sie sicher, dass Sie einen IAM-Benutzer verwenden, der Zugriff auf Lightsail hat.
- Wenn Ihr IAM-Benutzer keinen Zugriff auf Lightsail hat, wenden Sie sich an den Rootbenutzer des AWS-Kontos oder an einen IAM-Benutzer mit Administratorzugriff, um einen Zugang zu Lightsail zu beantragen. Weitere Informationen finden Sie unter Verwalten des Zugriffs auf Amazon Lightsail für einen IAM-Benutzer.
- Wenn Sie weiterhin den Fehler 403 erhalten, nachdem Sie die oben genannten Schritte versucht haben, wenden Sie sich bitte an den AWS-Support. In einigen seltenen Fällen für AWS-Konten, die vor 2011 erstellt wurden, muss der Support Ihr Konto manuell bei Lightsail abonnieren.

Beheben von Lightsail-Datenträgerproblemen

Unter Umständen treten in Lightsail Fehler bei den Blockspeicherdatenträgern auf. In diesem Thema werden allgemeine Probleme identifiziert und Umgehungen für diese Fehler empfohlen.

Allgemeine Datenträgerfehler

Suchen Sie unten nach der besten Beschreibung für Ihr Problem. Folgen Sie den Links, um den Fehler zu beheben. Wenn der aufgetretene Fehler nicht in der Liste enthalten ist, klicken Sie unten auf dieser Seite auf den Link Questions? (Haben Sie Fragen?) Der Link Kommentare? befindet sich am Ende dieser Seite, um Feedback zu geben oder den AWS Support zu kontaktieren.

Ich kann einen Datenträger nicht löschen, da er immer noch an eine Instance angefügt ist.

> Versuchen Sie, zuerst den Datenträger von der Instance zu trennen. Löschen Sie den Datenträger danach. Weitere Informationen finden Sie unter Trennen und Löschen von Blockspeicherdatenträgern.

Original-Fehlermeldung: You can't perform this operation because the disk is still attached to a Lightsail-instance (Sie können diese Operation nicht ausführen, da der Datenträger noch einer Lightsail-Instance zugewiesen ist): ***YOUR_INSTANCE (IHRE_INSTANCE)***

Mein Datenträger hat den Status „error“.

Der Fehlerstatus weist darauf hin, dass die zu Ihrem Datenträger Lightsail gehörende Hardware ausgefallen ist. Sie können den Datenträger aus einem aktuellen Snapshot wiederherstellen, andernfalls können die mit dem Datenträger verknüpften Daten nicht wiederhergestellt werden. Weitere Informationen finden Sie unter Erstellen eines Blockspeicher-Datenträgers von einem Snapshots.

Datenträger mit dem Status error werden Ihnen nicht in Rechnung gestellt.

Ich kann einen Datenträger nicht trennen, da die Lightsail-Instance immer noch ausgeführt wird.

Versuchen Sie, zuerst die Instance anzuhalten und dann den Datenträger zu trennen. Weitere Informationen finden Sie unter Anhalten einer Instance.

Original-Fehlermeldung: You can't detach this disk right now (Sie können diesen Datenträger momentan nicht trennen). Der Status des Datenträgers ist: ***DATENTRÄGER_STATUS***

Ich kann keine benutzerdefinierte Datenträgergröße über 16 TB (16.384 GB) angeben.

Versuchen Sie, einen kleineren Datenträger zu erstellen. Zusätzliche Datenträger können bis zu 16 TB groß sein. Wenn Ihr Datenträger kleiner als 16 TB ist und Sie ihn dennoch nicht erstellen können, tritt möglicherweise der nächste Fehler in der Liste auf (zu viele große Datenträger). Der Grund hierfür ist, dass der zusätzliche Datenträgerspeicher in Ihrem gesamten AWS-Konto auf 20 TB begrenzt ist. Weitere Informationen finden Sie unter Blockspeicherdatenträger.

Original-Fehlermeldung: The size of a block storage disk must be between 8 and 16384 GB (Die Größe eines Blockspeicherdatenträgers muss zwischen 8 und 16384 GB betragen).

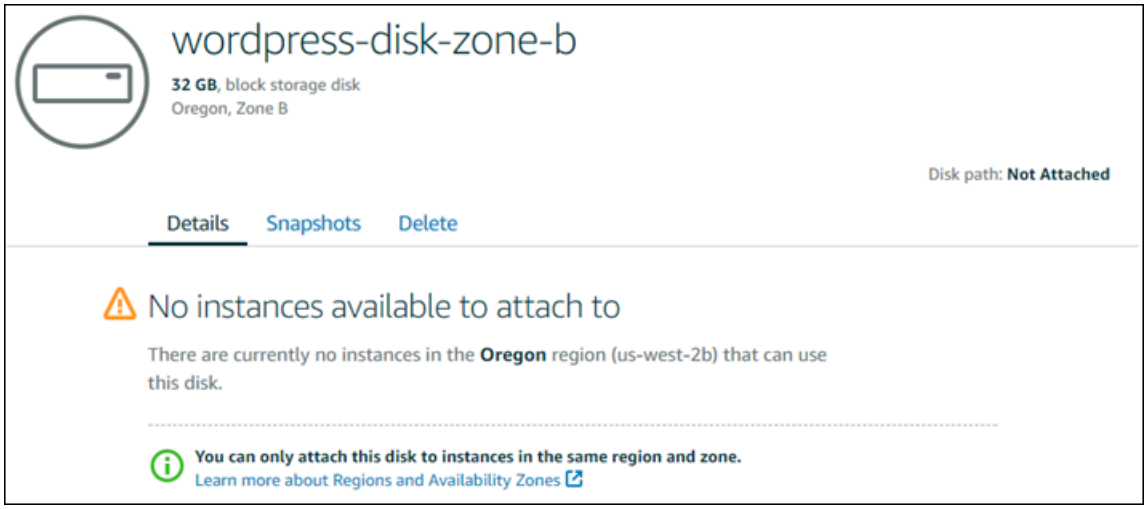
Ich kann keine weiteren Datenträger in Lightsail erstellen.

Möglicherweise haben Sie das Kontingent für die Anzahl von Datenträgern ausgeschöpft, die Sie erstellen können. Oder Sie haben möglicherweise zu viele große Datenträger in Ihrem AWS-Konto erstellt (die Gesamtgröße des Datenträgerspeichers darf 20 TB nicht überschreiten). Weitere Informationen finden Sie unter Blockspeicherdatenträger.

Tatsächliche Fehlermeldung:Sie haben die maximale Größe aller Datenträger dieses Kontos erreicht. oder Sie haben die maximale Anzahl von Datenträgern in diesem Konto erreicht.

Ich kann meiner Lightsail-Instance den Datenträger nicht anfügen.

Wenn der folgende Fehler auftritt, müssen Sie den Datenträger erneut erstellen, und zwar in derselben AWS-Region und -Availability Zone wie die Instance, der Sie den Datenträger anfügen möchten.



Original-Fehlermeldung: There are currently no instances in the (Es gibt keine Instances in ***AWS Region*** that can use this disk (die den Datentäger nutzen können).

Beheben von Verbindungsproblemen mit dem browserbasierten Lightsail-SSH- oder RDP-Client

Möglicherweise erhalten Sie eine Fehlermeldung, wenn Sie versuchen, eine Verbindung zu einer Instance über die browserbasierten SSH- oder RDP-Clients herzustellen, die in der Amazon Lightsail-Konsole verfügbar sind. Die möglichen Ursachen für diesen Fehler werden in den folgenden Abschnitten erläutert.

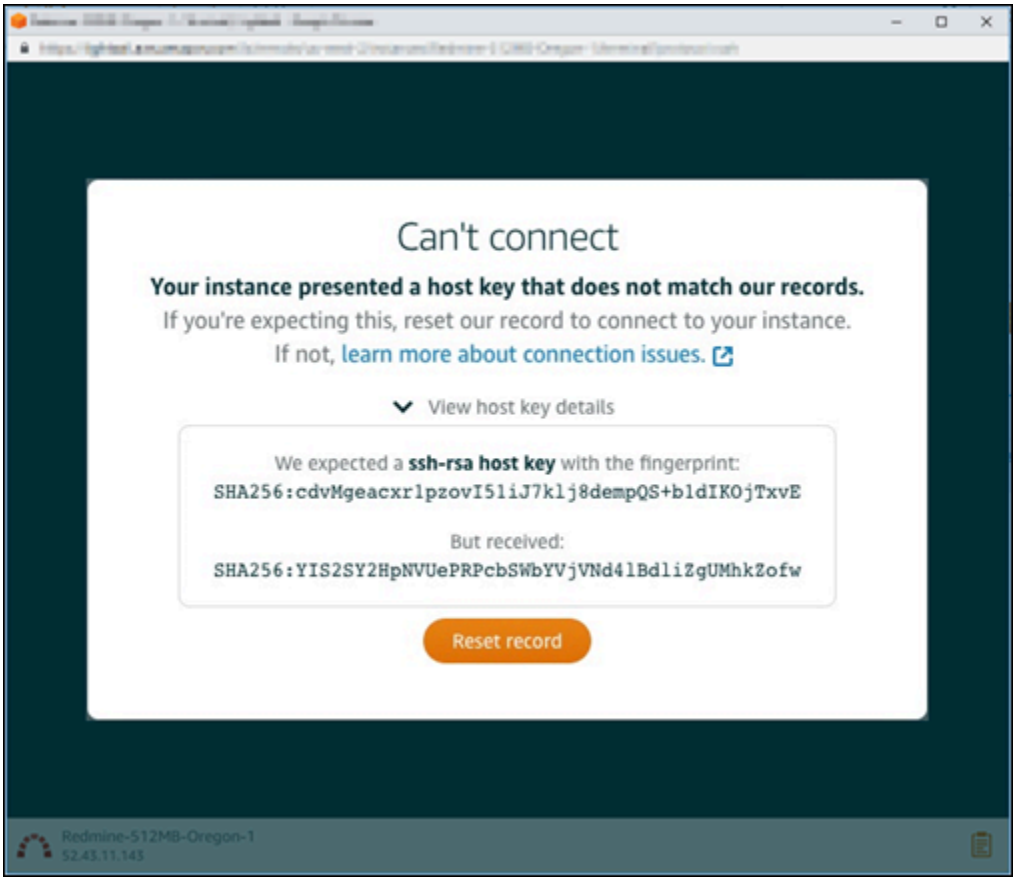
> **Important**
>
> Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um SSH oder RDP über IPv6 in Ihre Instance zu übertragen. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

Fehlermeldung: Verbindung kann nicht hergestellt werden

Der SSH- und RDP-Browser-basierte Client verwendet Host-Schlüssel oder Zertifikatvalidierung zur Authentifizierung einer Instance, wenn er eine Verbindung zu ihr herstellen will. Wenn die Instance einen Hostschlüssel oder ein Zertifikat präsentiert, das nicht mit dem von Lightsail aufgezeichneten übereinstimmt, wird eine von zwei Fehlermeldungen angezeigt. Beide Fehlermeldungen werden in diesem Abschnitt beschrieben.

Verbindung kann nicht hergestellt werden, Datensatz zurücksetzen

Die folgende Fehlermeldung wird angezeigt, wenn ein Hostschlüssel oder ein Zertifikat nicht übereinstimmen und Lightsail feststellt, dass die Nichtübereinstimmung möglicherweise durch ein aktuelles Betriebssystem-Upgrade oder eine bewusste Aktualisierung des Hostschlüssels oder des Zertifikats durch Sie oder einen anderen Benutzer verursacht wurde. In diesem Fall hat Lightsail festgestellt, dass der Hostschlüssel oder die Zertifikatsabweichung nicht durch einen fehlerhaften Akteur im Netzwerk zwischen Ihrem Browser und der Instance verursacht wurde.



Wählen Sie Reset record (Datensatz zurücksetzen), wenn Sie den Übereinstimmungsfehler erwartet haben. Diese Aktion löscht den Hostschlüssel oder das Zertifikat, das Lightsail für die Instance

gespeichert hat, und erlaubt der browserbasierten SSH- oder RDP-Sitzung, eine Verbindung mit der Instance herzustellen.

Sie können auch den Hostschlüssel oder das Zertifikat löschen, das Lightsail in Ihrem Datensatz hat, indem Sie den folgenden AWS Command Line Interface (AWS CLI)-Befehl verwenden. Geben Sie für den Namen Ihrer Instance ein*InstanceName*, für die Sie den bekannten Hostschlüssel oder das Zertifikat löschen möchten. Geben Sie für *Region* die AWS-Region der Instance ein.

```
aws lightsail delete-known-host-keys --region Region --instance-name InstanceName
```

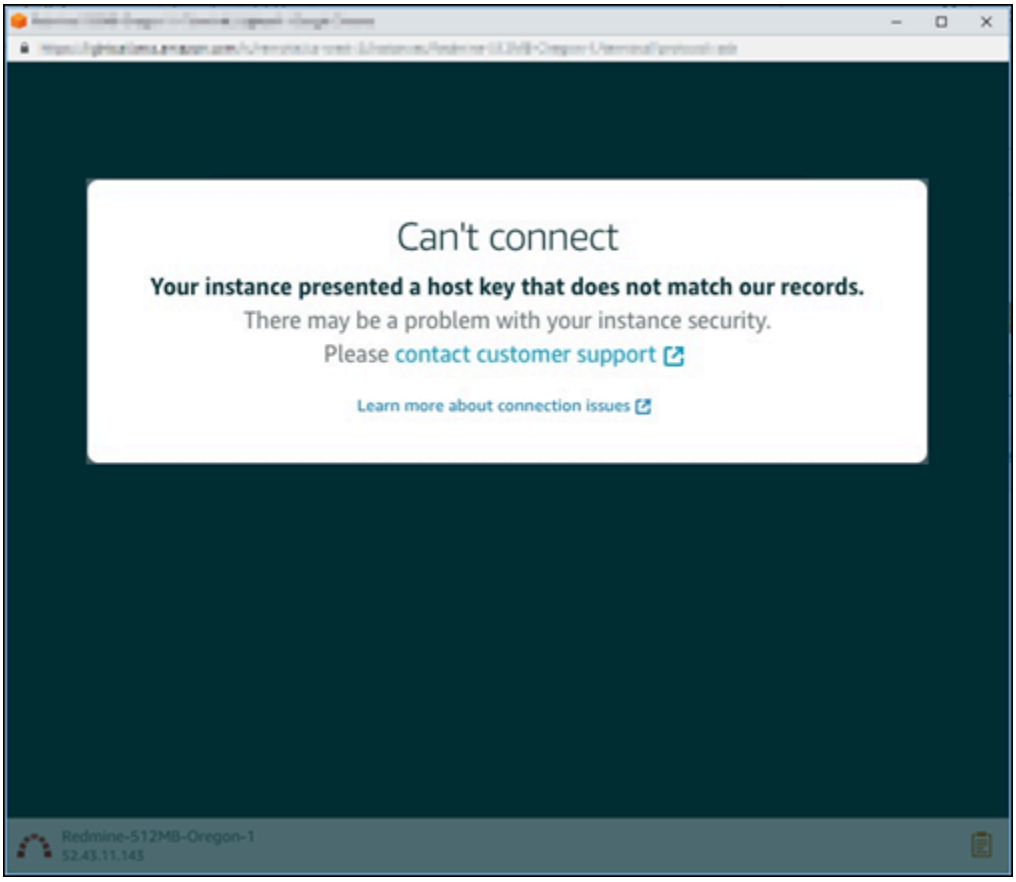
Beispiel:

```
aws lightsail delete-known-host-keys --region us-west-2 --instance-
name WordPress-512MB-Oregon-1
```

> **Note**
>
> Weitere Informationen zur finden Sie AWS CLIunter Konfigurieren der AWS CLI für die Arbeit mit Lightsail.

Verbindung kann nicht hergestellt werden, wenden Sie sich an den Kunden-Support

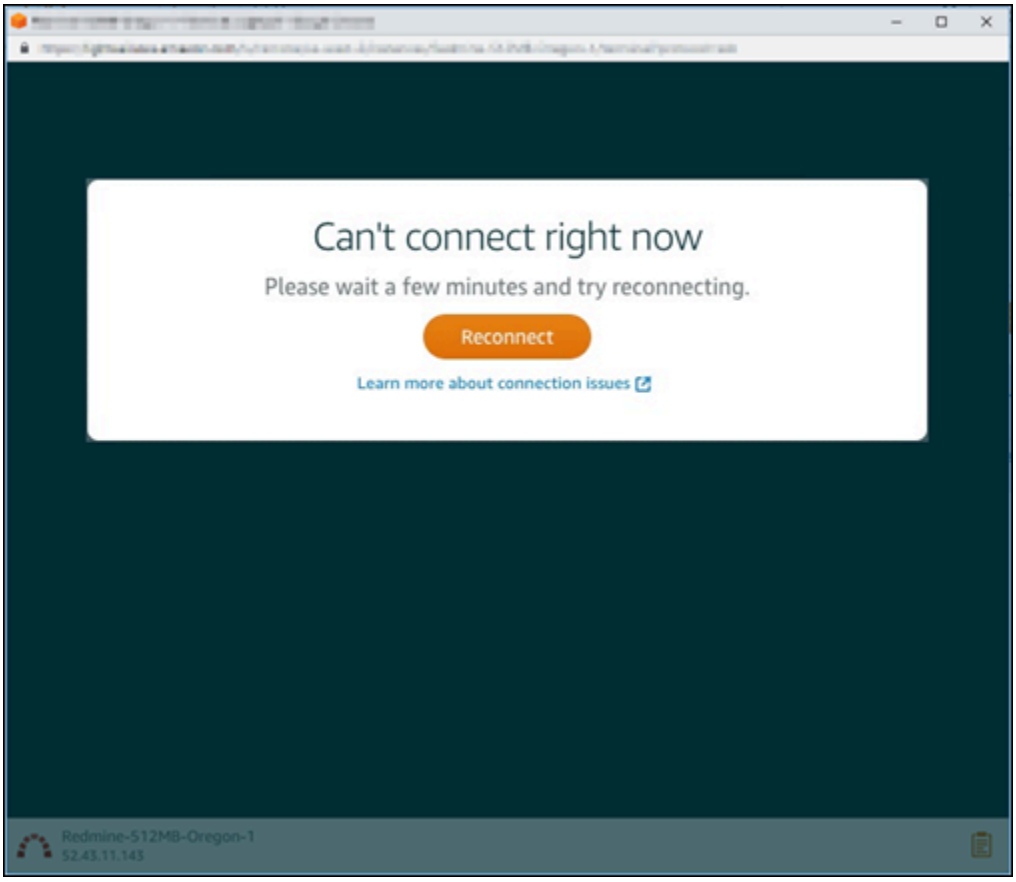
Die folgende Fehlermeldung wird angezeigt, wenn ein Hostschlüssel oder eine Zertifikatsabweichung vorliegt und Lightsail feststellt, dass verdächtige Aktivitäten vorliegen, die eine weitere Untersuchung erfordern, z. B. ein man-in-the-middle Angriff.



Diese Fehlermeldung bedeutet, dass Sie keine Verbindung mit der Instance mithilfe des Browser-basierten SSH- oder RDP-Clients herstellen können. Wenden Sie sich an den Support, wenn Sie Hilfe benötigen.

Fehlermeldung: Die Verbindung kann derzeit nicht hergestellt werden

Die folgende Fehlermeldung wird angezeigt, wenn Sie versuchen, sich mit einer Instance zu verbinden, die nach dem Erstellen, Reboot oder Neustart noch nicht gestartet wurde. Warten Sie einige Minuten und klicken Sie dann auf Reconnect (Neu verbinden), um es erneut zu versuchen.



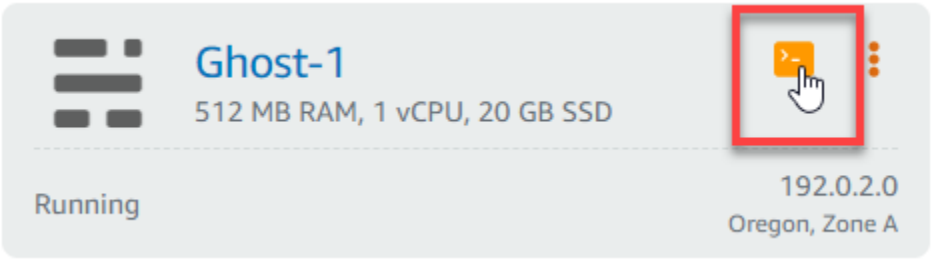
Wenn Sie immer noch keine Verbindung herstellen können, wenden Sie sich an den AWS-Support.

Fehlerbehebung zu „503 service unavailable“ für eine Ghost-Instance in Lightsail

Nachdem Sie eine neue Ghost-Instance in Amazon Lightsail erstellt haben und versuchen, auf Ihre Website zuzugreifen, wird möglicherweise ein Fehler angezeigt, der besagt, dass der Service nicht verfügbar ist (503). In einigen Fällen wird der Ghost-Service beim Erstellen der Instance nicht automatisch auf der Instance gestartet. Dies kann passieren, wenn Sie das Bundle 3,50 USD/Monat für Ihre Instance auswählen. Gehen Sie folgendermaßen vor, um den Ghost-Service zu starten und den Fehler „service is unavailable“ (Service ist nicht verfügbar) zu beheben.

Starten des Ghost-Services

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Instances.
3. Klicken Sie auf das browserbasierte SSH-Client-Symbol für Ihre Ghost-Instance.



4. Nachdem der SSH-Client verbunden ist, geben Sie den folgenden Befehl ein, um alle Services auf der Instance neu zu starten:

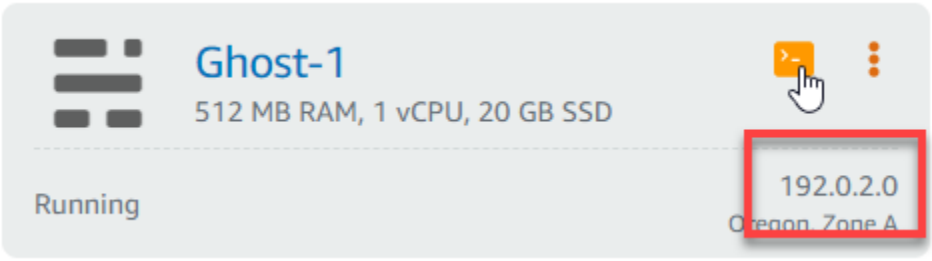
```
sudo /opt/bitnami/ctlscript.sh restart
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:

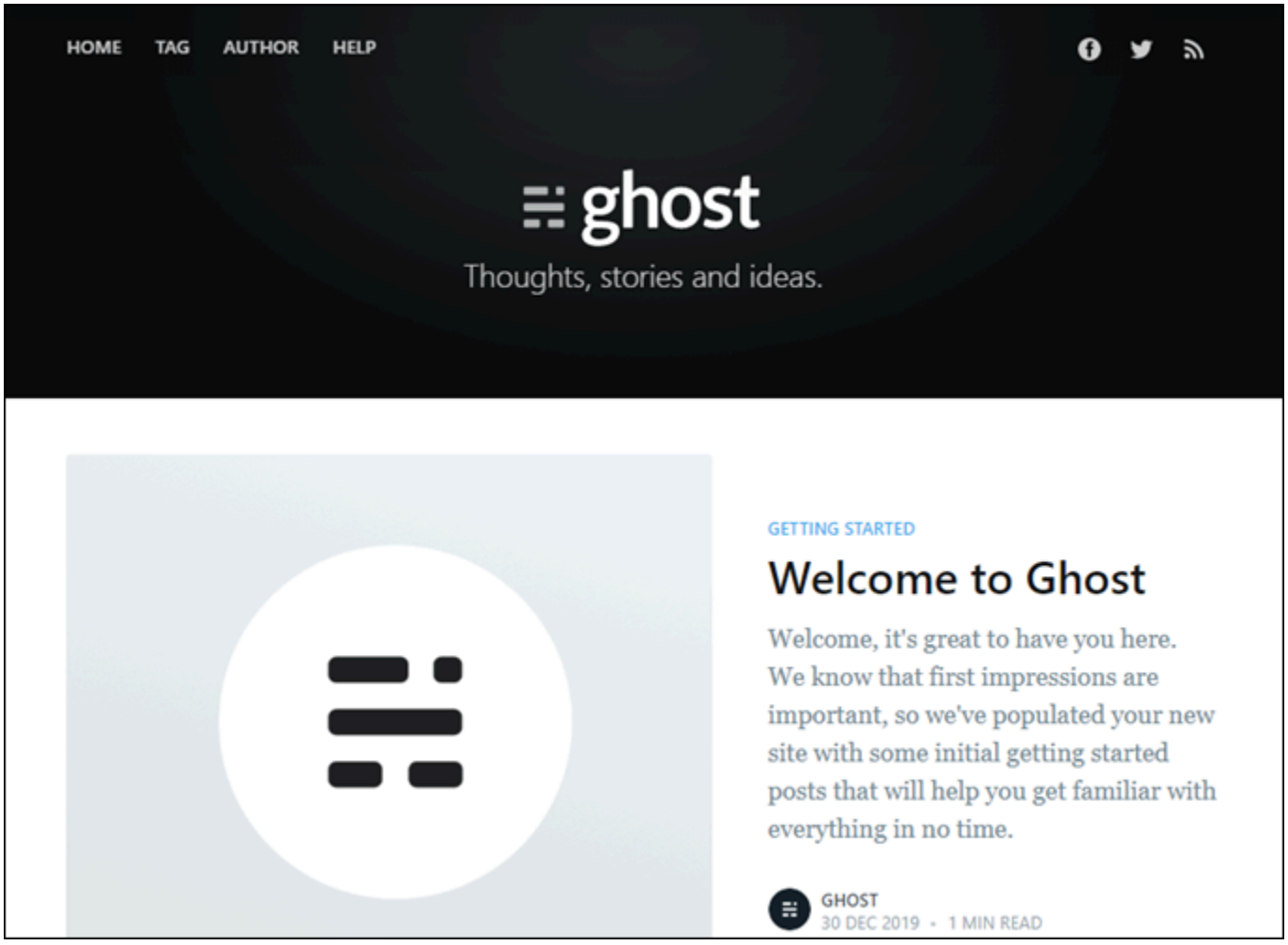
```
bitnami@ip-172-26-11-214:~$ sudo /opt/bitnami/ctlscript.sh restart
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd stopped
/opt/bitnami/apps/ghost/scripts/ctl.sh : ghost not running
/opt/bitnami/mysql/scripts/ctl.sh : mysql stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql  started at port 3306
» Ensuring user is not logged in as ghost user [skipped]
» Checking if logged in user is directory owner [skipped]
✔ Checking current folder permissions
✔ Validating config
✔ Checking memory availability
✔ Checking binary dependencies
✔ Starting Ghost: 127-0-0-1

------------------------------------------------------------------------------

Your admin interface is located at:

    http://18.237.117.48:80/ghost/

/opt/bitnami/apps/ghost/scripts/ctl.sh : ghost started
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd started at port 80
```

5. Navigieren Sie zur öffentlichen IP-Adresse Ihrer Instance, um zu bestätigen, dass Ihre Ghost-Website verfügbar ist und ausgeführt wird.

   Die öffentliche IP-Adresse Ihrer Instance wird neben dem Instance-Namen auf der Registerkarte Instances der Lightsail-Konsole aufgeführt.



Wenn Sie zur öffentlichen IP-Adresse Ihrer neuen Ghost-Instance navigieren, sollten Sie die standardmäßige Ghost-Website-Vorlage sehen:



Fehlerbehandlung für Identity and Access Management (IAM) in Lightsail

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit Lightsail und IAM auftreten könnten.

Ich bin nicht autorisiert, eine Aktion in Lightsail auszuführen.

Wenn die AWS Management Console Ihnen mitteilt, dass Sie nicht zur Ausführung einer Aktion autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort bereitgestellt hat.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, auf die Lightsail-Konsole zuzugreifen, aber keine `lightsail:*` (Vollzugriffs)-Berechtigungen hat.

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um ihm den Zugriff auf die Lightsail-Konsole mit den `lightsail:*`(-Vollzugriffs)-Berechtigungen zu ermöglichen.

Ich bin nicht zur Ausführung von iam:PassRole autorisiert

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Ausführung der Aktion `iam:PassRole` autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an Amazon Lightsail übergeben zu können.

Einige AWS-Services erlauben die Übergabe einer vorhandenen Rolle an diesen Service, sodass keine neue Servicerolle oder serviceverknüpfte Rolle erstellt werden muss. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Service.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Amazon Lightsail auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen odzur Verfügung gestellt.

Ich möchte meine Zugriffsschlüssel anzeigen

Nachdem Sie Ihre IAM-Benutzerzugriffsschlüssel erstellt haben, können Sie Ihre Zugriffsschlüssel-ID jederzeit anzeigen. Sie können Ihren geheimen Zugriffsschlüssel jedoch nicht erneut anzeigen. Wenn Sie den geheimen Zugriffsschlüssel verlieren, müssen Sie ein neues Zugriffsschlüsselpaar erstellen.

Zugriffsschlüssel bestehen aus zwei Teilen: einer Zugriffsschlüssel-ID (z. B. `AKIAIOSFODNN7EXAMPLE`) und einem geheimen Zugriffsschlüssel (z. B. `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Ähnlich wie bei Benutzernamen und Passwörtern müssen Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zusammen verwenden, um Ihre Anforderungen zu authentifizieren. Verwalten Sie Ihre Zugriffsschlüssel so sicher wie Ihren Benutzernamen und Ihr Passwort.

> **Important**
>
> Geben Sie Ihre Zugriffsschlüssel nicht an Dritte weiter, auch nicht für die Suche nach Ihrer kanonischen Benutzer-ID. Wenn Sie dies tun, gewähren Sie anderen Personen möglicherweise den permanenten Zugriff auf Ihr AWS-Konto.

Während der Erstellung eines Zugriffsschlüsselpaars werden Sie aufgefordert, die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel an einem sicheren Speicherort zu speichern. Der geheime Zugriffsschlüssel ist nur zu dem Zeitpunkt verfügbar, an dem Sie ihn erstellen. Wenn Sie Ihren geheimen Zugriffsschlüssel verlieren, müssen Sie Ihrem IAM-Benutzer neue Zugriffsschlüssel hinzufügen. Sie können maximal zwei Zugriffsschlüssel besitzen. Wenn Sie bereits zwei Zugriffschlüssel besitzen, müssen Sie ein Schlüsselpaar löschen, bevor Sie ein neues erstellen. Anweisungen hierfür finden Sie unter Verwalten von Zugriffsschlüsseln im IAM-Benutzerhandbuch.

Ich bin Administrator und möchte anderen Zugriff auf Lightsail gewähren.

Um anderen Personen oder einer Anwendung Zugriff auf Amazon Lightsail zu gewähren, müssen Sie eine IAM-Entität (Benutzer oder Rolle) für die Person oder Anwendung erstellen, die Zugriff benötigt. Sie werden die Anmeldeinformationen für diese Einrichtung verwenden, um auf AWS zuzugreifen. Anschließend müssen Sie der Entität eine Richtlinie anfügen, die dieser die korrekten Berechtigungen in Amazon Lightsail gewährt.

Informationen zum Einstieg finden Sie unter Erstellen Ihrer ersten delegierten IAM-Benutzer und -Gruppen im IAM-Benutzerhandbuch.

Ich möchte Personen außerhalb meines AWS-Kontos Zugriff auf meine Lightsail-Ressourcen erteilen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Amazon Lightsail diese Funktionen unterstützt, finden Sie unter Funktionsweise von Amazon Lightsail mit IAM.

- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Überprüfen der IPv6-Erreichbarkeit in Lightsail

Sie können die IPv6-Konnektivität von Ihrem lokalen Computer zu einer Amazon Lightsail-Instance mithilfe des Ping-Tools überprüfen. Ping ist ein Netzwerkdiagnosedienstprogramm, das zur Behebung von Verbindungsproblemen zwischen zwei oder mehr Netzwerkgeräten verwendet wird. Wenn Ping erfolgreich ist, sollten Sie in der Lage sein, eine Verbindung zu Ihrer Instance über IPv6 herzustellen. Wenn eine Netzwerkeinstellung oder ein Gerät nicht so konfiguriert ist, dass IPv6 zugelassen wird, schlägt der Ping-Befehl fehl. Weitere Informationen finden Sie unter Überlegungen zu IPv6.

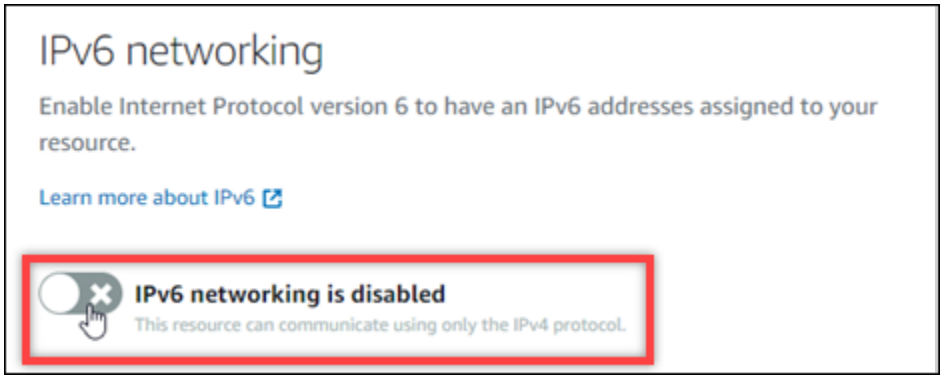
Inhalt

Aktivieren von IPv6 für Dual-Stack-Instances

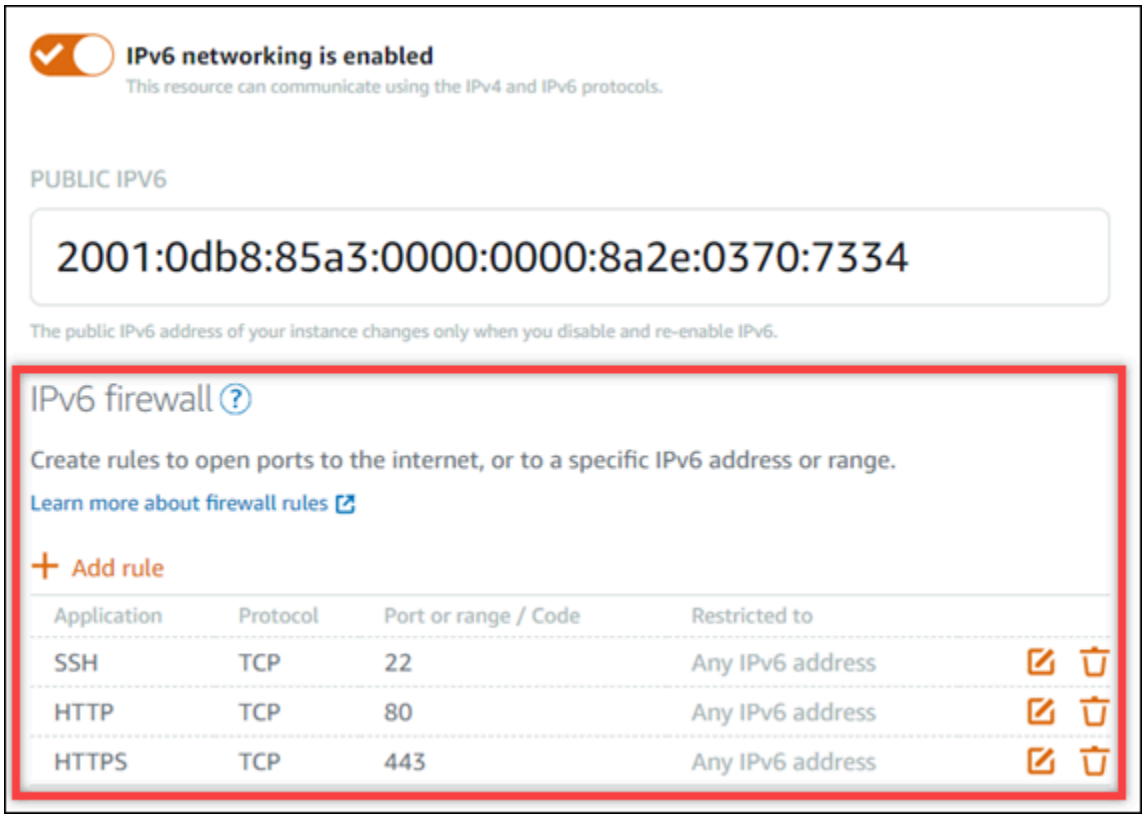
Aktivieren Sie IPv6 für Ihre Dual-Stack-Instance, bevor Sie mit dem Testen beginnen. IPv6 ist für IPv6-onlyInstances immer aktiviert.

Vervollständigen Sie das folgende Verfahren, um IPv6 auf Ihrer Dual-Stack-Instance zu aktivieren, wenn es nicht aktiviert ist.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie den Namen der Instance aus, für die Sie IPv6 aktivieren möchten. Stellen Sie sicher, dass Ihre Instance ausgeführt wird.
3. Wählen Sie auf der Instance-Verwaltungsseite die Registerkarte Netzwerk aus.
4. Aktivieren Sie IPv6 im Abschnitt IPv6-Netzwerk der Seite.



Nachdem Sie IPv6 aktiviert haben, wird Ihrer Instance eine öffentliche IPv6-Adresse zugewiesen, und die IPv6-Firewall wird verfügbar.



5. Notieren Sie sich oben auf der Seite die öffentlichen IPv4- und öffentlichen IPv6-Adressen der Instance. Sie werden sie in den folgenden Abschnitten verwenden.

Konfigurieren der Firewall der Instance

Die Firewall in der Lightsail-Konsole fungiert als virtuelle Firewall. Dies bedeutet, dass gesteuert wird, welcher Datenverkehr über seine öffentliche IP-Adresse eine Verbindung zu Ihrer Instance herstellen darf. Jede Dual-Stack-Instance, die Sie in Lightsail erstellen, verfügt über eine individuelle Firewall für IPv4-Adressen und eine weitere für IPv6-Adressen. Jede Firewall enthält eine Reihe von Regeln, die den Datenverkehr filtern, der in die Instance eingeht. Beide Firewalls sind voneinander unabhängig – Sie müssen Firewallregeln für IPv4 und IPv6 separat konfigurieren. Instances mit einem IPv6-only-Plan verfügen über keine IPv4-Firewall, die Sie konfigurieren können.

Führen Sie das folgende Verfahren aus, um die Firewall Ihrer Instance für Internet Control Message Protocol (ICMP)-Datenverkehr zu konfigurieren. Das Ping-Dienstprogramm verwendet das ICMP-Protokoll, um mit Ihrer Instance zu kommunizieren. Weitere Informationen finden Sie unter Instance-Firewalls in Amazon Lightsail.

> **Important**
>
> Windows und Linux enthalten eine Firewall auf Betriebssystemebene (OS), die Ping-Befehle blockieren kann. Stellen Sie sicher, dass die Betriebssystem-Firewall der Instance ICMP-Datenverkehr über IPv4 und IPv6 akzeptieren kann, bevor Sie fortfahren. Weitere Informationen finden Sie in der folgenden -Dokumentation:
>
> - Herstellen einer Verbindung mit Ihrer Lightsail-Windows-Instance
> - Herstellen einer Verbindung zu Ihren Lightsail-Linux- oder Unix-Instances

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie den Namen der Instance aus, für die Sie die Firewall konfigurieren möchten.
3. Wählen Sie auf der Instance-Verwaltungsseite die Registerkarte Netzwerk und führen Sie dann die verbleibenden Schritte im entsprechenden Abschnitt für den Firewall-Typ aus, den Sie verwenden möchten. Führen Sie für IPv4 die Schritte im Abschnitt IPv4-Firewall aus. Führen Sie für IPv6 die Schritte im Abschnitt IPv6-Firewall aus.

   a. Wählen Sie im Dropdown-Menü Anwendung die Option Ping (ICMP) aus.

   b. Aktivieren Sie das Feld Auf IP-Adresse beschränken, um eine Verbindung von Ihrer lokalen Quell-IP-Adresse oder Ihrem lokalen Quell-IP-Bereich zuzulassen, und geben Sie dann Ihre Quell-IP-Adresse ein. (Optional) Sie können das Feld deaktiviert lassen, um eine

Verbindung von jeder IP-Adresse aus zuzulassen. Wir empfehlen, diese Option nur in einer Testumgebung zu verwenden.

c. Wählen Sie Erstellen, um die neue Regel auf Ihre Instance anzuwenden.

Testen der Erreichbarkeit für Ihre Instance

Führen Sie das folgende Verfahren aus, um die IPv4- oder IPv6-Erreichbarkeit von Ihrem lokalen Computer oder Netzwerk zu Ihrer Lightsail-Instance zu testen. Sie benötigen die öffentlichen IPv4- und IPv6-Adressen der Instance, die Sie in notiert habenStep 5.

Von einem Linux-, Unix- oder macOS-Gerät

1. Öffnen Sie ein Terminalfenster auf Ihrem lokalen Gerät.
2. Geben Sie einen der folgenden Befehle ein, um einen Ping an Ihre Lightsail-Instance zu senden. Ersetzen Sie die Beispiel-IP-*Adresse*, die im Befehl enthalten ist, durch die öffentliche IPv4- oder IPv6-Adresse Ihrer Instance.

   So testen Sie über IPv4

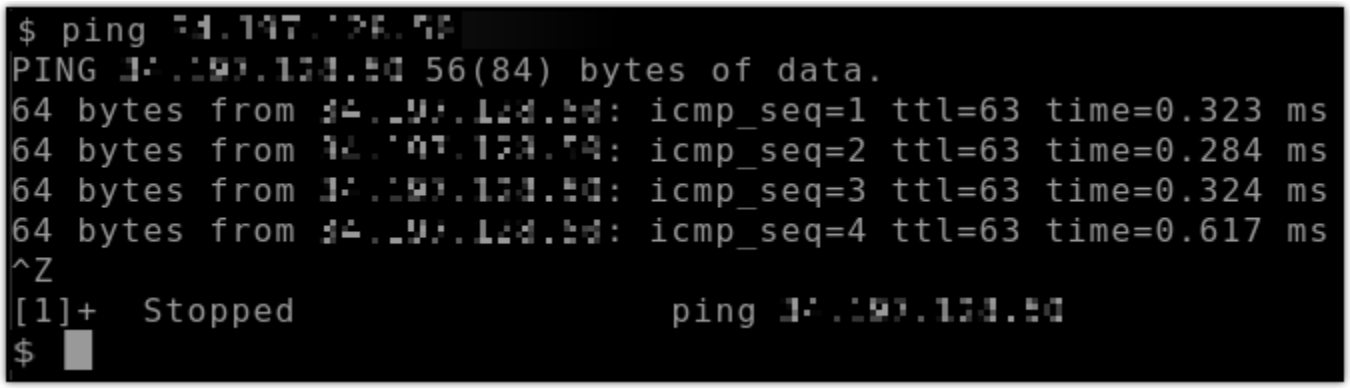
   ```
   ping 192.0.2.0
   ```

   So testen Sie über IPv6

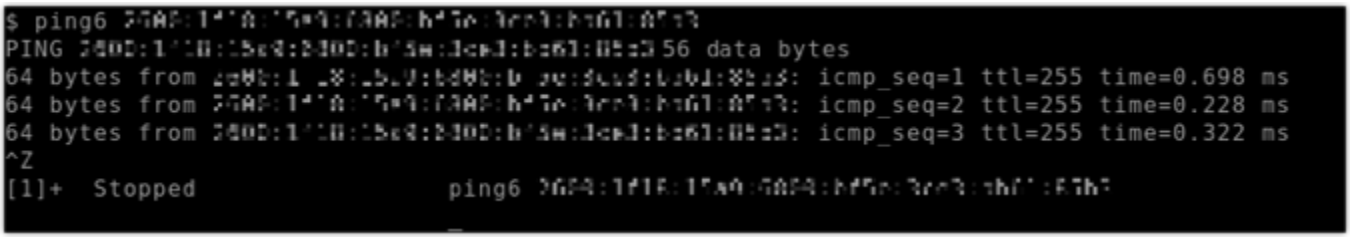
   ```
   ping6 2001:db8::
   ```

3. Nachdem der Befehl einige Antworten zurückgegeben hat, geben Sie `ctrl+z` auf der Tastatur Ihres Geräts ein, um den Befehl zu beenden.

Der Ping-Befehl gibt erfolgreiche Antworten von der IPv4-Adresse Ihrer Instance zurück, wenn er erfolgreich ist. Das Ergebnis sollte wie folgt aussehen:



Der Befehl ping6 gibt erfolgreiche Antworten von der IPv6-Adresse Ihrer Instance zurück, wenn er erfolgreich ist. Das Ergebnis sollte wie folgt aussehen:



Beide Befehle geben das Anforderungs-Timeout zurück, wenn Ihre Instance nicht erreicht werden kann.

Von einem Windows-Gerät

1. Öffnen Sie eine Befehlszeile.
2. Geben Sie einen der folgenden Befehle ein, um einen Ping an Ihre Lightsail-Instance zu senden. Ersetzen Sie die Beispiel-IP-*Adresse*, die im Befehl enthalten ist, durch die öffentliche IPv4- oder IPv6-Adresse Ihrer Instance.

   So testen Sie über IPv4

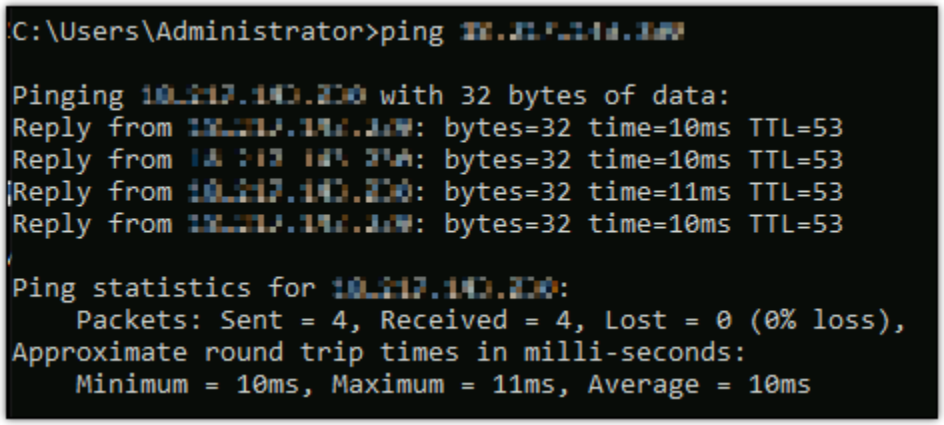
   ```
   ping 192.0.2.0
   ```

   So testen Sie über IPv6

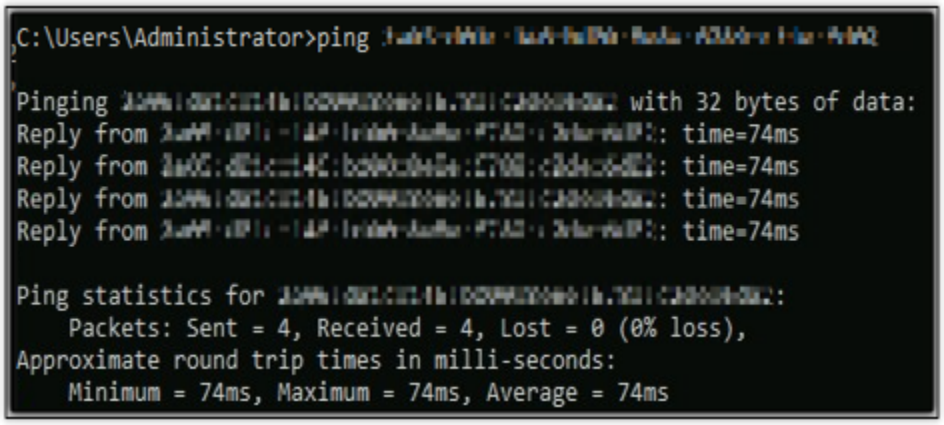
   ```
   ping 2001:db8::
   ```

3. Nachdem der Befehl einige Antworten zurückgegeben hat, geben Sie `ctrl+z` auf der Tastatur Ihres Geräts ein, um den Befehl zu beenden.

Der Ping-Befehl gibt erfolgreiche Antworten von der IPv4-Adresse Ihrer Instance zurück, wenn er erfolgreich ist. Das Ergebnis sollte wie folgt aussehen:



Der Ping-Befehl gibt erfolgreiche Antworten von der IPv6-Adresse Ihrer Instance zurück, wenn er erfolgreich ist. Das Ergebnis sollte wie folgt aussehen:



Beide Befehle geben das Anforderungs-Timeout zurück, wenn Ihre Instance nicht erreicht werden kann.

Ungenügende Kapazität der Instance in Lightsail

Wenn Sie versuchen, eine Instance zu starten oder eine gestoppte Instance neu zu starten, erhalten Sie möglicherweise die Fehlermeldung „unzureichend“. Das bedeutet, dass AWS derzeit nicht über die Instance-Kapazität verfügt, um Ihre Anfrage zu erfüllen. Nachfolgend finden Sie ein Beispiel für den Fehler bei unzureichender Instance-Kapazität:

InsufficientInstanceCapacity: Es ist nicht genug Kapazität vorhanden, um Ihre Instance-Anforderung zu erfüllen. Reduzieren Sie die Anzahl der Instances in Ihrer Anforderung oder warten Sie, bis

zusätzliche Kapazität verfügbar wird. Sie können auch versuchen, eine Instance zu starten, indem Sie ein kleineres Lightsail-Preismodell auswählen (die Größe können Sie später anpassen).“

In diesem Handbuch erfahren Sie, welche Maßnahmen Sie ergreifen können, wenn ein Fehler mit unzureichender Instance-Kapazität auftritt.

Inhalt

Unzureichende Kapazität beim Starten einer neuen Instance

Verwenden Sie die folgenden Optionen, wenn beim Starten einer neuen Instance ein Fehler mit unzureichender Instance-Kapazität angezeigt wird. Sie können jede Option der Reihe nach abschließen oder eine Option auswählen, die für Sie funktioniert.

1. Warten Sie einige Minuten und senden Sie Ihre Anfrage erneut. Die Instance-Kapazität kann häufig wechseln. Fahren Sie mit Option 2 fort, wenn Sie Ihre Instance nach einigen Minuten nicht erstellen können.
2. Wählen Sie eine andere Availability Zone (AZ), wenn Sie Ihre Instance erstellen. Jede AWS-Region enthält drei oder mehr AZs, und jede AZ verfügt über unterschiedliche Instance-Kapazitäten. Wenn Sie eine andere AZ auswählen, können Sie die Vorteile von der aktuellen Instance-Kapazität nutzen. Fahren Sie mit Option 3 fort, wenn Sie keine Instance in einer anderen AWS-Region oder AZ erstellen können.
3. Reduzieren Sie die Anzahl der Instances in Ihrer Anforderung. Wenn Sie mehrere Instances gleichzeitig erstellen, reduzieren Sie die Anzahl der Instances und reichen Sie Ihre Anfrage erneut ein. Fahren Sie mit Option 4 fort, wenn das Problem durch die Reduzierung der Anzahl der Instances nicht behoben wird.
4. Wählen Sie bei der Erstellung Ihrer Instance einen anderen Instance-Plan. Wählen Sie einen anderen instance-Plan, wenn Sie keine Instance in einer anderen AZ oder Region erstellen können. Sie können die Größe der Instance zu einem späteren Zeitpunkt ändern. Weitere Informationen zur Größenanpassung Ihrer Instance finden Sie unter Erstellen einer Instance aus einem Snapshot.

Unzureichende Kapazität beim Starten einer gestoppten Instance

Verwenden Sie die folgenden Optionen, wenn beim Starten einer vorhandenen Instance, die zuvor gestoppt wurde, ein Fehler mit unzureichender Instance-Kapazität angezeigt wird.

1. Warten Sie einige Minuten und senden Sie Ihre Anfrage erneut. Die Instance-Kapazität kann häufig wechseln. Fahren Sie mit Option 2 fort, wenn Sie Ihre Instance nach einigen Minuten nicht erstellen können.
2. Erstellen einer neuen Instance aus einem Snapshot. Erstellen Sie einen Snapshot der gestoppten Instance. Verwenden Sie dann den Snapshot, um eine neue Instance in einer AZ zu erstellen, die sich von der ursprünglichen Instance unterscheidet. Wenn sich Ihre Instance beispielsweise derzeit in us-east-2a (Zone A) befindet, wählen Sie us-east-2c (Zone C) aus, wenn Sie die neue Instance erstellen. Weitere Informationen finden Sie unter Erstellen einer Instance aus einem Snapshot.
3. Sie können auch einen anderen Instance-Plan wählen, wenn Sie eine neue Instance aus einem Snapshot erstellen. Dieser Schritt ist optional.

> **Important**
>
> Sobald die neue Instance ausgeführt wird, überprüfen Sie, ob Sie Zugriff auf die neue Instance haben. Wenn auf Ihrer Instance beispielsweise eine Anwendung ausgeführt wurde, stellen Sie sicher, dass die Anwendung wie erwartet funktioniert. In diesem Fall können Sie die frühere Instance löschen.

Ähnliche Informationen

Häufig gestellte Fragen

Ausfallsicherheit in Lightsail

Fehlerbehebung bei Lightsail-Load Balancern

Es kann zu Fehlern bei Ihren Lightsail-Load Balancern kommen. In diesem Thema werden allgemeine Probleme identifiziert und Umgehungen für diese Fehler empfohlen.

Allgemeine Load Balancer-Fehler

Suchen Sie unten nach der besten Beschreibung für Ihr Problem. Folgen Sie den Links, um den Fehler zu beheben. Wenn der aufgetretene Fehler nicht in der Liste enthalten ist, klicken Sie unten auf dieser Seite auf den Link Questions? (Haben Sie Fragen?) Kommentare? Der Link befindet sich am Ende dieser Seite, um Feedback zu geben oder den AWS-Kundenservice zu kontaktieren.

Ich kann kein Zertifikat erstellen.

Es gibt ein Kontingent für Anzahl der Zertifikate, die Sie in einem AWS-Konto erstellen können. Weitere Informationen finden Sie unter Kontingente im AWS Certificate Manager-Benutzerhandbuch. Die gleichen Kontingente gelten für Lightsail-Zertifikate für Load Balancer.

Original-Fehlermeldung: Sorry, you've requested too many certificates for your account (Sie haben zu viele Zertifikate für Ihr Konto angefordert).

Ich kann meinem Load Balancer keine weiteren Instances anfügen.

Sie können Ihrem Load Balancer beliebig viele Lightsail-Instances anfügen, solange Sie sich innerhalb des Kontigents von insgesamt 20 Lightsail-Instances pro AWS-Konto bewegen.

Original-Fehlermeldung: Sorry, you've reached the maximum number of instances you can attach to this load balancer (Sie haben die maximale Anzahl an Instances, die an den Load Balancer angefügt werden können, erreicht).

Ich kann meinem Load Balancer eine bestimmte Instance nicht anfügen.

Überprüfen Sie zunächst, ob Ihre Lightsail-Instance ausgeführt wird. Wenn sie angehalten ist, können Sie sie über die Instance-Management-Seite starten. Lightsail-Instances müssen ausgeführt werden, um einem Load Balancer angefügt werden zu können.

Es kann sein, dass eine Instance an zu viele Load Balancer angefügt ist.

Original-Fehlermeldung: Sorry, you've reached the maximum number of times an instance can be registered with a load balancer (Sie haben die maximale Anzahl, an denen eine Instance mit dem Load Balancer registriert werden kann, erreicht).

Lightsail kann die Instance nicht finden, die ich dem Load Balancer anfügen möchte

Möglicherweise versuchen Sie, eine Instance zuzuweisen, die nicht mehr existiert oder sich nicht in derselben VPC wie die Zielgruppe befindet.

Original-Fehlermeldung: Sorry, the instance you specified doesn't exist, isn't in the same VPC as the target group, or has an unsupported instance type (Die Instance, die Sie spezifiziert haben, existiert nicht, ist nicht in der selben VPC wie die Zielgruppe oder der Instance-Typ wird nicht unterstützt).

Fehlerbehebungs-Benachrichtigungen in Lightsail

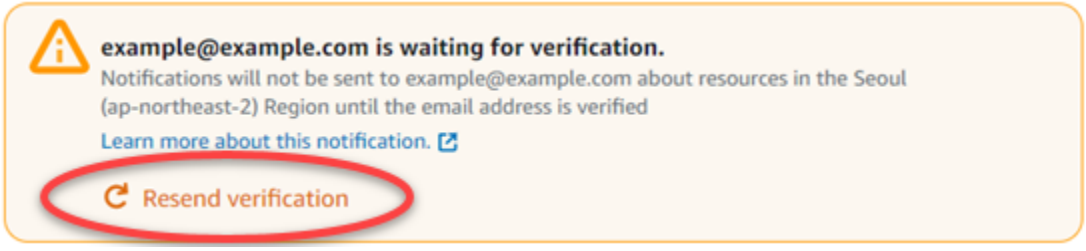
Wenn Sie wider Erwarten keine Benachrichtigungen erhalten, müssen Sie einige Punkte überprüfen, um sicherzustellen, dass Ihre Benachrichtigungskontakte korrekt konfiguriert sind. Weitere Informationen zu Benachrichtigungen finden Sie unter Benachrichtigungen.

In der folgenden Liste sind häufige Probleme mit Benachrichtigungskontakten sowie die Ursachen und entsprechenden Lösungen aufgeführt. Wenn der aufgetretene Fehler nicht in der Liste enthalten ist, klicken Sie unten auf dieser Seite auf den Link Haben Sie Fragen? Der Link Kommentare? befindet sich am Ende dieser Seite, um Feedback zu geben oder das AWS Support-Center zu kontaktieren.

Ich habe meine E-Mail-Adresse als Benachrichtigungskontakt hinzugefügt, aber ich erhalte keine E-Mail-Benachrichtigungen

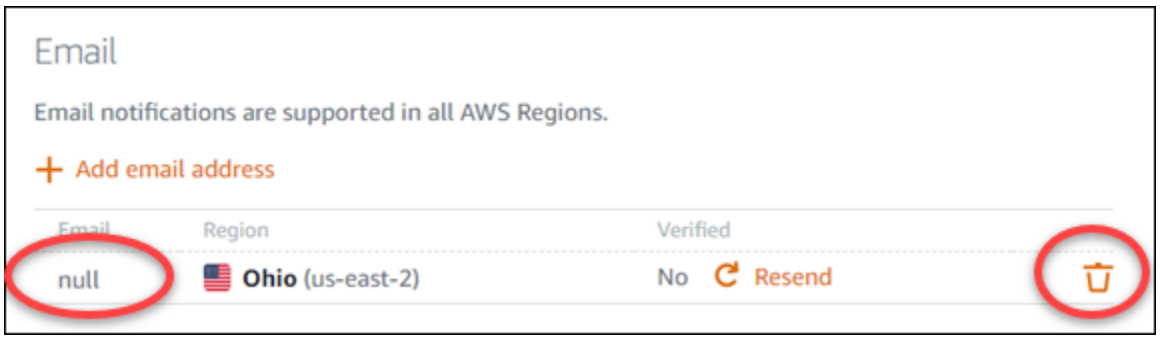
Wenn Sie eine E-Mail-Adresse als Benachrichtigungskontakt in Lightsail hinzufügen, wird eine Verifizierungsanfrage an diese Adresse gesendet. Die Bestätigungs-E-Mail enthält einen Link, auf den der Empfänger klicken muss, um den gewünschten Erhalt von Lightsail-Benachrichtigungen zu bestätigen. Benachrichtigungen werden erst nach der Verifizierung an die E-Mail-Adresse gesendet. Die Verifizierung erhalten Sie von AWS-Benachrichtigungen <no-reply@sns.amazonaws.com> und der Betreff lautet AWS-Benachrichtigung-Abonnement-Bestätigung. Für SMS-Nachrichten ist keine Verifizierung erforderlich.

Überprüfen Sie die Spam- und Junk-Ordner des Postfachs, wenn sich die Bestätigungs-E-Mail nicht im Posteingang befindet. Wenn die Verifizierungsanforderung verloren gegangen ist oder gelöscht wurde, wählen Sie Verifizierung erneut senden im Benachrichtigungsbanner, das in der Lightsail-Konsole und in der Seite Kontoangezeigt wird.



null (Null) ist als mein E-Mail-Benachrichtigungskontakt aufgeführt.

E-Mail-Adressen müssen innerhalb von 24 Stunden nach dem Hinzufügen verifiziert werden. Wenn Sie eine E-Mail nicht innerhalb von 24 Stunden verifizieren, erhält diese E-Mail automatisch den Status `invalid` und wird von Lightsail entfernt. Aus diesem Grund wird möglicherweise der Wert null (Null) für einen oder mehrere Ihrer E-Mail-Benachrichtigungskontakte angezeigt.



Um dieses Problem zu beheben, entfernen Sie den null (Null)-E-Mail-Benachrichtigungskontakt und fügen Sie die richtige E-Mail-Adresse erneut hinzu. Sie müssen die E-Mail-Adresse sofort nach dem Hinzufügen zu Lightsail verifizieren. Weitere Informationen finden Sie unter Benachrichtigungen.

Ich habe keine SMS-Benachrichtigungen erhalten oder ich bekomme seit Neuestem keine mehr

Möglicherweise haben Sie sich vom Empfang von SMS-Benachrichtigungen abgemeldet. Sie können sich abmelden, indem Sie auf eine SMS-Benachrichtigung mit `ARRET` (Französisch), `CANCEL`, `END`, `OPT-OUT`, `OPTOUT`, `QUIT`, `REMOVE`, `STOP`, `TD` oder `UNSUBSCRIBE` antworten. Wenn Sie eine Mobiltelefonnummer entfernen, müssen Sie 30 Tage warten, bevor Sie diese Mobiltelefonnummer erneut als Benachrichtigungskontakt in Lightsail hinzufügen können.

Fehlerbehebung bei SSL/TLS-Zertifikaten in Lightsail

Es kann zu Fehlern bei Ihren Lightsail-Load Balancern kommen. In diesem Thema werden allgemeine Probleme identifiziert und Umgehungen für diese Fehler empfohlen.

Suchen Sie unten nach der besten Beschreibung für Ihr Problem. Folgen Sie den Links, um den Fehler zu beheben. Wenn der aufgetretene Fehler nicht in der Liste enthalten ist, klicken Sie unten auf dieser Seite auf den Link Questions? (Haben Sie Fragen?) Kommentare? Der Link befindet sich am Ende dieser Seite, um Feedback zu geben oder den AWS-Kundenservice zu kontaktieren.

Ich kann kein Zertifikat erstellen.

Es gibt ein Kontingent für Anzahl der Zertifikate, die Sie in einem AWS-Konto erstellen können. Weitere Informationen finden Sie unter Kontingente im AWS Certificate Manager-Benutzerhandbuch. Die gleichen Kontingente gelten für Lightsail-Zertifikate für Load Balancer.

Original-Fehlermeldung: Sorry, you've requested too many certificates for your account (Sie haben zu viele Zertifikate für Ihr Konto angefordert).

Meine Zertifikatsanforderung ist fehlgeschlagen.

Wenn die Zertifikatsanforderung fehlgeschlagen ist, können Sie den Vorgang mit Retry (Nochmal versuchen) auf der Registerkarte Inbound traffic (Eingehender Datenverkehr) der Load Balancer-Verwaltungsseite wiederholen.

Wenn Sie die Fehlerursache nicht ermitteln können, wenden Sie sich bitte an den AWS-Kundenservice.

Mein Domäne wurde als ungültig angezeigt.

Wenn Sie Probleme haben, zu prüfen, ob Sie eine Domäne kontrollieren, vergewissern Sie sich, dass Sie Zugriff auf die DNS-Verwaltung haben. Wenn dies der Fall ist, Sie diese Anweisungen befolgt haben und das Problem weiterhin besteht, wenden Sie sich bitte an den AWS-Kundenservice.

Amazon Lightsail-Anleitungen

Die folgenden Tutorials führen Sie durch gängige Amazon Lightsail-Anwendungsfälle. In diesen Tutorials erfahren Sie beispielsweise, wie Sie Fehler in Lightsail beheben und wie Sie sie Lightsail zusammen mit anderen AWS-Services verwenden. Darüber hinaus können Sie lernen, wie Sie mit den verschiedenen Lightsail-Vorlagen wie Bitnami, WordPress, LAMP oder Windows Server arbeiten.

Themen

Schnellstart-Anleitungen für Amazon Lightsail

Verwenden Sie die folgenden Schnellstart-Anleitungen, um mit Lightsail-Vorlagen zu beginnen. In Lightsail ist eine Vorlage ein virtuelles Abbild, das bereits mit einem Betriebssystem und einer Anwendung geliefert wird. Die Anwendungen umfassen WordPress, WordPress Multisite, cPanel und WHM, PrestaShop, Drupal, Ghost, Joomla!, Magento, Redmine, LAMP, Nginx (LEMP) und Node.js

Themen

- Schnellstartanleitung: Plesk
- Schnellstartanleitung: PrestaShop
- Schnellstartanleitung: Redmine
- Schnellstartanleitung: WordPress
- Schnellstartanleitung: WordPress Multisite

Schnellstart: cPanel und WHM

Hier sind einige erste Schritte, die Sie unternehmen sollten, nachdem Ihre cPanel & WHM-Instance auf Amazon Lightsail hochgefahren ist und läuft.

> **Important**
>
> Ihre cPanel & WHM-Instance enthält eine 15-Tage-Testlizenz. Nach 15 Tagen müssen Sie eine Lizenz von cPanel erwerben, um weiterhin cPanel & WHM verwenden zu können. Wenn Sie eine Lizenz erwerben möchten, führen Sie die Schritte 1-7 dieses Leitfadens aus, bevor Sie Ihre Lizenz erwerben.

Inhalt

Schritt 1: Ändern des Passworts des Root-Benutzers

Führen Sie das folgende Verfahren aus, um das Stammbenutzer-Passwort für Ihre cPanel-Instance zu ändern. Verwenden Sie den Stammbenutzer und das Passwort, um sich später bei der Web Host Manager (WHM) -Konsole anzumelden.

1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).
2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um das Anwendungspasswort zu erhalten:

   ```
   sudo passwd
   ```

3. Geben Sie ein sicheres Passwort ein und bestätigen Sie es, indem Sie es ein zweites Mal eingeben.

   > **Note**
   >
   > Ihr Passwort sollte keine Wörterbuchwörter enthalten und sollte mehr als 7 Zeichen enthalten. Wenn Sie diese Richtlinien nicht befolgen, erhalten Sie eine`BAD PASSWORD`-Warnung.

   Beachten Sie dieses Passwort, da Sie es für die Anmeldung bei der WHM-Konsole zu einem späteren Zeitpunkt in diesem Leitfaden verwenden.

Schritt 2: Fügen Sie an Ihre cPanel & WHM-Instance eine statische IP-Adresse an

Die standardmäßig an Ihre Instance angefügte dynamische öffentliche IP-Adresse ändert sich bei jedem Stopp und Start der Instance. Erstellen Sie eine statische IP-Adresse und fügen Sie sie an Ihre Instance an, damit die öffentliche IP-Adresse nicht mehr geändert wird. Später, wenn Sie Ihren Domainnamen mit Ihrer Instance verwenden, müssen Sie die DNS-Datensätze Ihrer Domain nicht jedes Mal aktualisieren, wenn Sie die Instance stoppen und starten. Wenn Ihre Instance ausfällt, können Sie Ihre Instance aus einem Backup wiederherstellen und Ihre statische IP Ihrer neuen Instance neu zuweisen. Sie können eine statische IP an eine Instance anhängen.

> **Important**
>
> Sie müssen die öffentliche IP-Adresse Ihrer cPanel & WHM-Instance angeben, wenn Sie eine Lizenz von cPanel erwerben. Die Lizenz, die Sie kaufen, ist dieser IP-Adresse zugeordnet. Aus diesem Grund müssen Sie eine statische IP an Ihre cPanel & WHM-Instance anhängen, wenn Sie eine Lizenz von cPanel erwerben möchten. Geben Sie Ihre statische IP an, wenn Sie eine Lizenz von cPanel erwerben, und behalten Sie Ihre statische IP so lange bei, wie Sie Ihre cPanel & WHM-Lizenz mit einer Lightsail-Instance verwenden möchten. Wenn Sie Ihre Lizenz später an eine andere IP-Adresse übertragen müssen, können Sie eine Anfrage an cPanel senden. Weitere Informationen finden Sie unter Übertragen einer Lizenz in der WHM-Dokumentation.

Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Networking (Netzwerk) die Option Create static IP (Statische IP erstellen) und folgen Sie dann den Anweisungen auf der Seite.

Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

Schritt 3: Melden Sie sich erstmals beim Web Host Manager an

Führen Sie das folgende Verfahren aus, um sich erstmals bei der WHM-Konsole anzumelden.

1. Öffnen Sie einen Webbrowser und navigieren Sie zu der folgenden Webadresse. Stellen Sie sicher, dass Sie *<StaticIP>* mit der neuen statischen IP-Adresse Ihrer Instance ersetzen. Fügen Sie unbedingt `:2087` an das Ende der Adresse, d. h. der Port, auf dem Sie eine Verbindung zu Ihrer Instance herstellen.

   ```
   https://<StaticIP>:2087
   ```

   Beispiel:

   ```
   https://192.0.2.0:2087
   ```

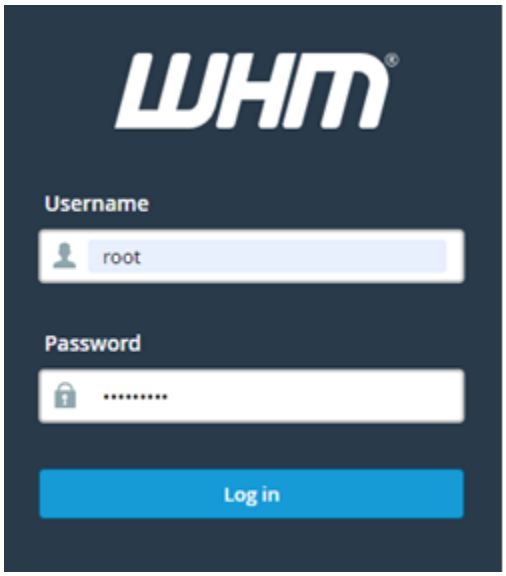
> **Important**
>
> Sie müssen `https://` in die Adressleiste Ihres Browsers einfügen, wenn Sie zur IP-Adresse und zum Port Ihrer Instance navigieren. Andernfalls erhalten Sie einen Fehler, der besagt, dass die Website nicht erreicht werden kann.

Wenn Sie beim Navigieren zur statischen IP-Adresse Ihrer Instance über Port 2087 keine Verbindung herstellen können, überprüfen Sie, ob Ihr Router, VPN oder Internetdienstanbieter HTTP/HTTPS-Verbindungen über Port 2087 zulässt. Wenn dies nicht der Fall ist, versuchen Sie, eine Verbindung über ein anderes Netzwerk herzustellen.

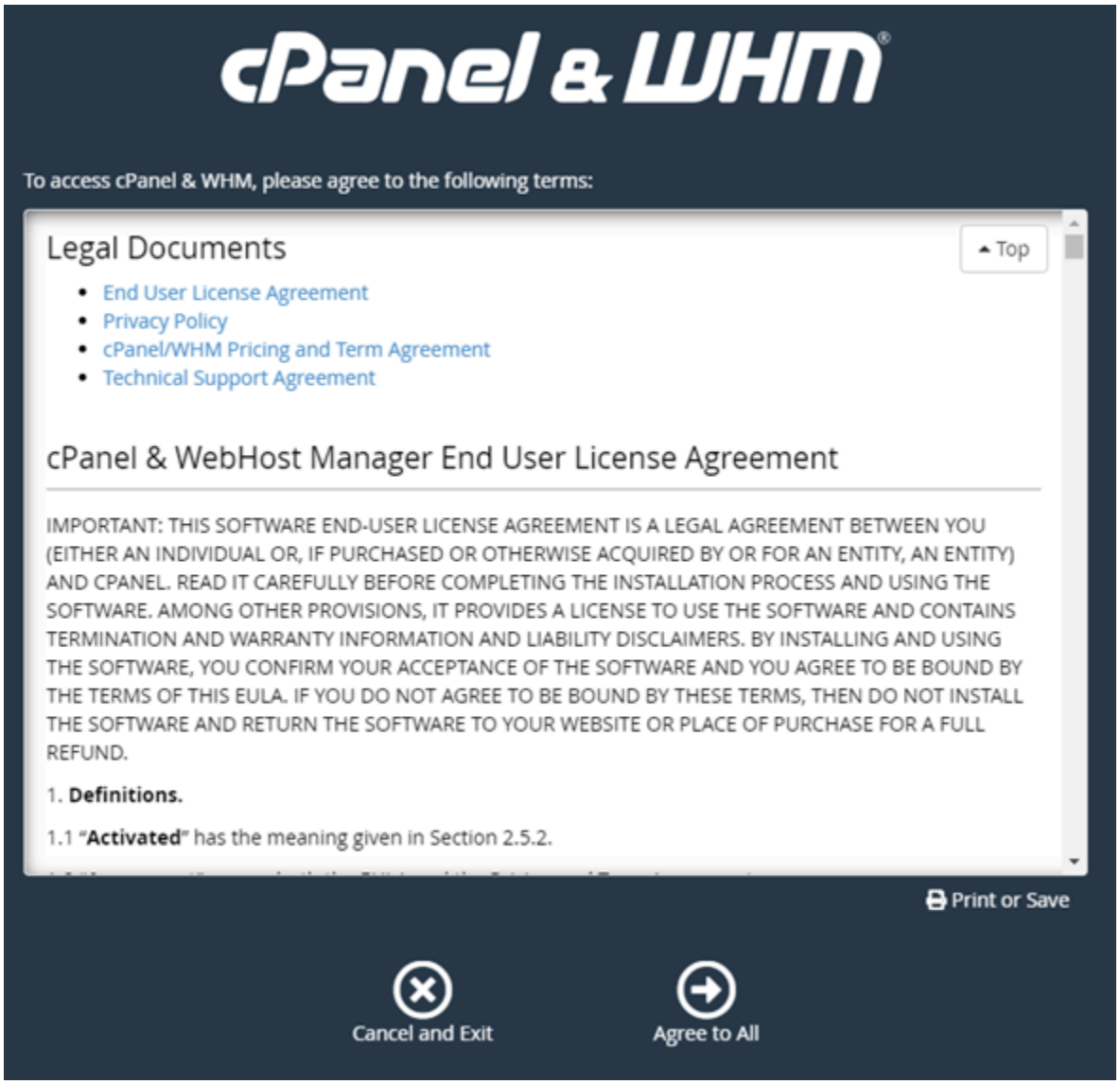
Möglicherweise warnt Ihr Browser Sie davor, dass Ihre Verbindung nicht privat bzw. sicher ist oder dass ein Sicherheitsrisiko besteht. Dies geschieht, weil Ihre cPanel-Instance noch nicht über eine SSL-/TLS-Zertifikat verfügt. Wählen Sie im Browserfenster Advanced (Erweitert) und dann Details oder More information (Weitere Informationen), um die verfügbaren Optionen anzuzeigen. Besuchen Sie dann die Website, auch wenn diese nicht privat oder sicher ist.

2. Geben Sie `root` in das Textfeld Benutzername ein.
3. Geben Sie das Root-Benutzerpasswort in das Textfeld Passwort ein.

   Dies ist das Passwort, das Sie zuvor in Abschnitt Schritt 1: Ändern des Passworts des Root-Benutzers in diesem Leitfaden angegeben haben.
4. Wählen Sie Log in (Anmelden).

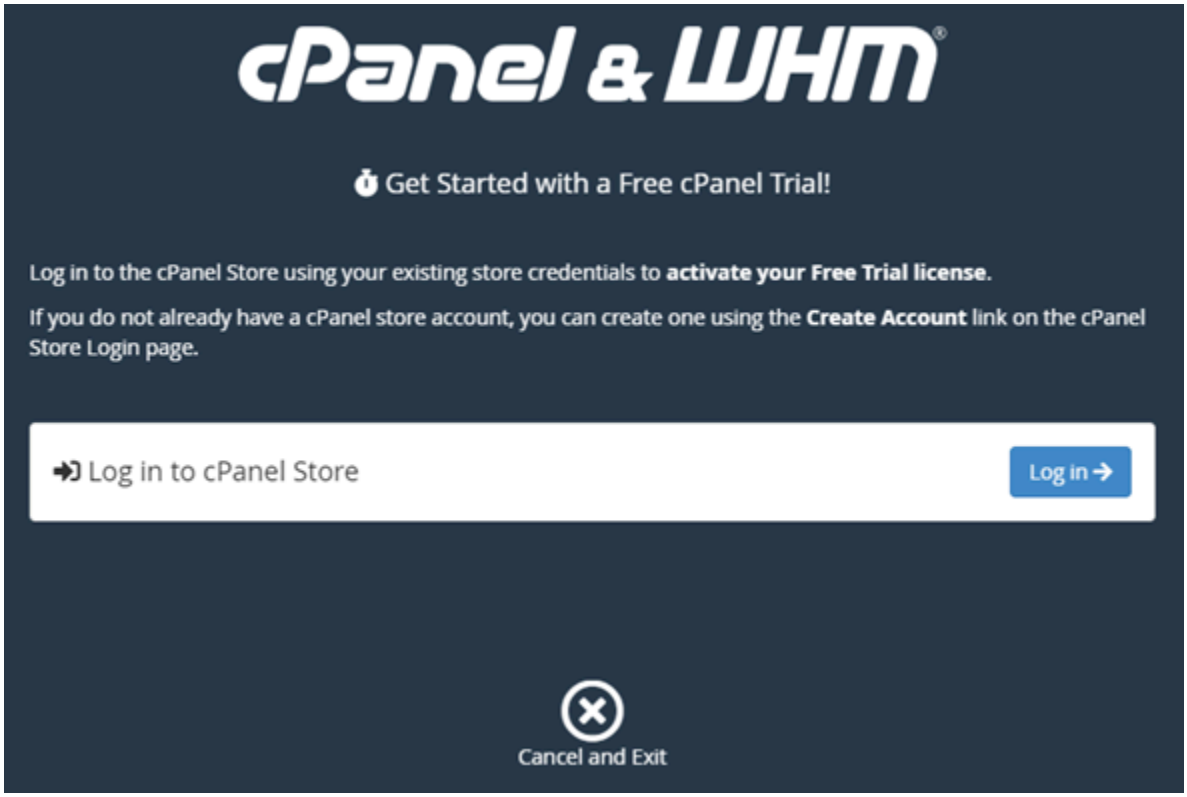


5. Lesen Sie die cPanel & WHM-Begriffe und wählen SieStimmen Sie allen zuWenn Sie fortfahren möchten.



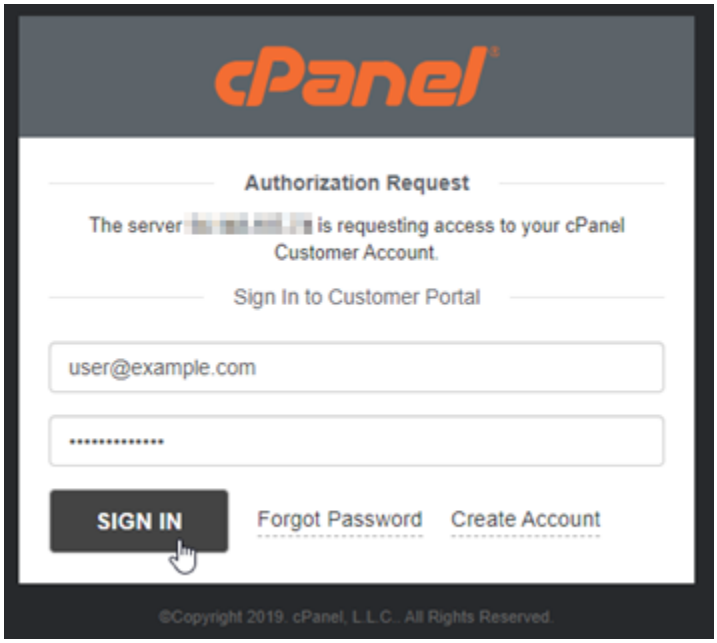
6. Wählen Sie auf der Seite Erste Schritte mit einer kostenlosen cPanel Testversion Anmelden bei, um sich beim cPanel-Speicher anzumelden.

   Sie müssen sich im cPanel-Store anmelden, um Ihre Testlizenz Ihrem Konto zuzuordnen. Wenn Sie über kein cPanel-Store-Konto verfügen, sollten SieAnmelden beiSie haben die Möglichkeit, eines zu erstellen.



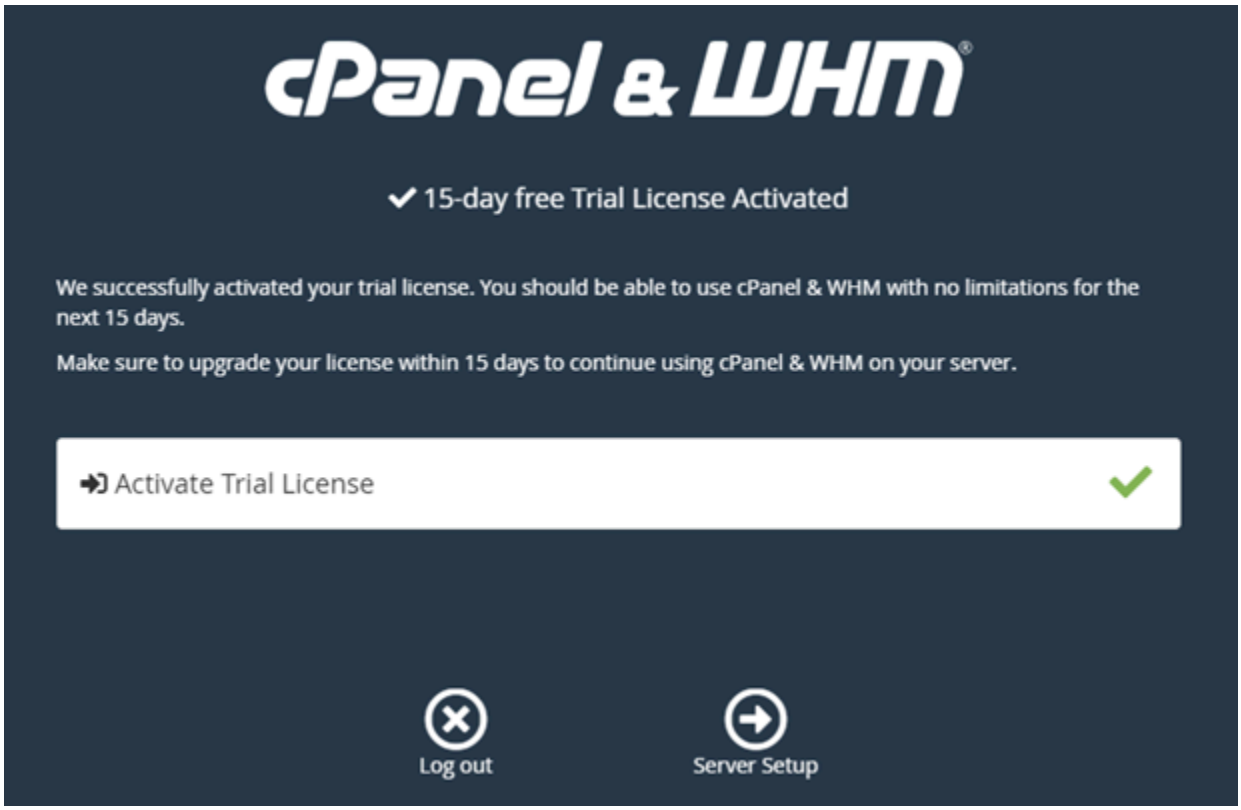
7. Auf der Seite Autorisierung beantragen, die angezeigt wird, geben Sie Ihre E-Mail-Adresse oder Ihren Benutzernamen und das Passwort für Ihr cPanel-Store-Konto ein.

   Wenn Sie über kein cPanel-Store-Konto verfügen, wählen Sie Erstellen eines Kontos und befolgen Sie die Anweisungen zum Erstellen Ihres neuen cPanel-Store-Kontos. Sie werden aufgefordert, Ihre E-Mail-Adresse einzugeben, und erhalten eine E-Mail, um Ihr cPanel- Store-Konto-Passwort festzulegen. Wir empfehlen, dass Sie Ihr cPanel Store-Konto-Passwort über einen neuen Browser-Tab festlegen. Wenn Ihr Passwort festgelegt ist, können Sie diese Registerkarte schließen und zu Ihrer Instance zurückkehren, um Ihr Konto zu autorisieren, und mit dem nächsten Schritt dieses Verfahrens fortfahren.
8. Klicken Sie auf Sign in.

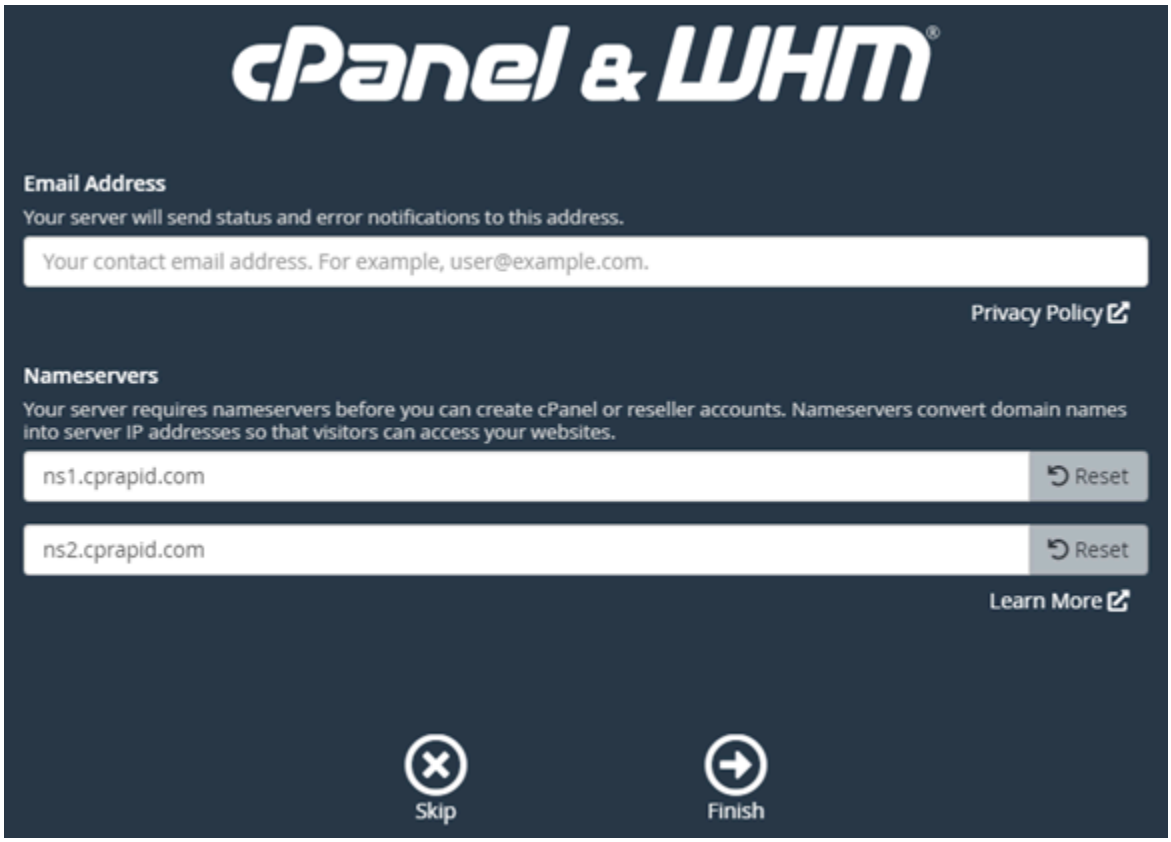


Nachdem Sie sich angemeldet haben, erhält Ihre cPanel & WHM-Instance eine 15-Tage-Testlizenz, die Ihrem cPanel Store-Konto zugeordnet ist. Gehen Sie zu Verwalten von Lizenzen im cPanel-Speicher, um Ihre ausgestellten Lizenzen, einschließlich Testlizenzen, anzuzeigen.

9. Klicken Sie auf Server-Setup, um fortzufahren.



10. Klicken Sie auf Übersprungen auf der Seite E-Mail-Adresse und Namenserver. Sie können diese später konfigurieren.

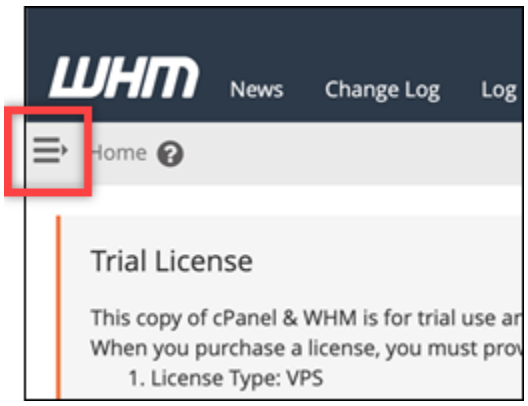


Die WHM-Konsole wird angezeigt, in der Sie die Einstellungen und Funktionen für cPanel verwalten können.

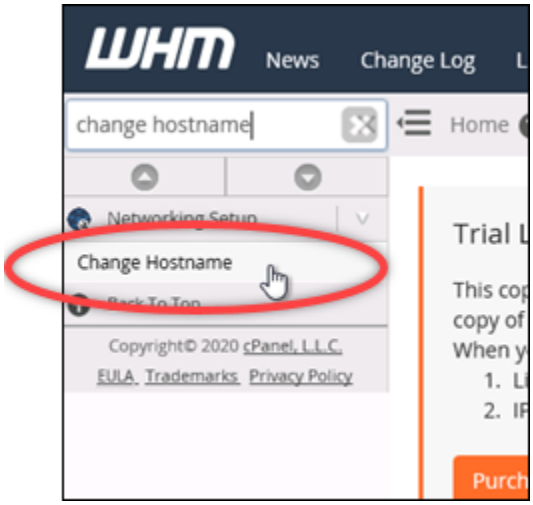
Schritt 4: Ändern des Hostnamens und der IP-Adresse Ihrer cPanel & WHM-Instance

Führen Sie die folgenden Schritte aus, um den Hostnamen Ihrer Instance zu ändern, sodass Sie nicht die öffentliche IP-Adresse für den Zugriff auf die WHM-Konsole verwenden müssen. Sie sollten die IP-Adresse Ihrer Instance auch in die neue statische IP-Adresse ändern, die Sie Ihrer Instance zuvor in Abschnitt Schritt 2: Anfügen einer statischen IP an Ihre cPanel & WHM-Instance in diesem Leitfaden angefügt haben.

1. Wählen Sie das Navigationsmenü-Symbol im oberen linken Bereich der WHM-Konsole.

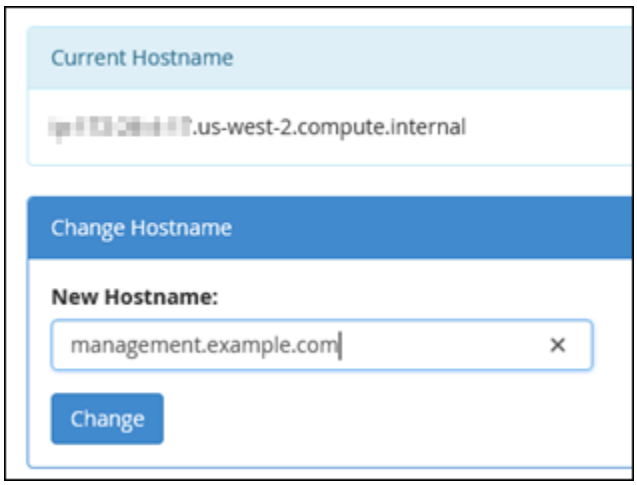


2. Geben Sie `Change hostname` im Suchtextfeld in der WHM-Konsole ein und wählen Sie dann die Option Ändern des Hostnamens in den Ergebnissen.

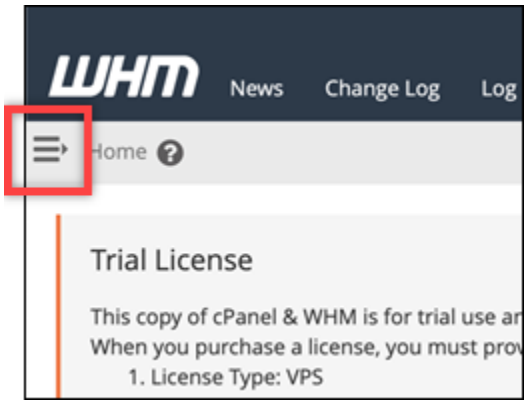


3. Geben Sie im Textfeld Neuer Hostname den Hostnamen ein, mit dem Sie auf die WHM-Konsole zugreifen möchten. Geben Sie beispielsweise `management.example.com` als `administration.example.com` ein.

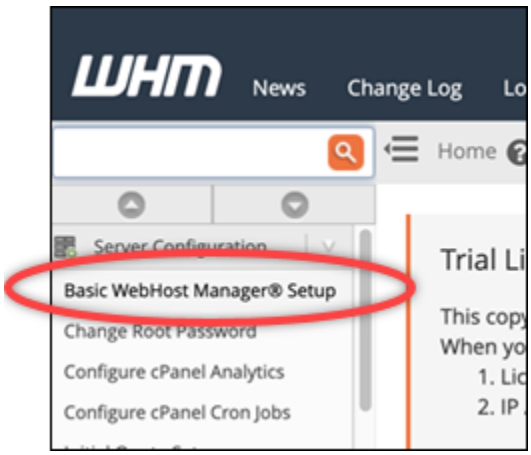
> **Note**
>
> Sie können nur eine Subdomain als Hostname angeben und Sie können nicht `whm` oder `cpanel` als Subdomäne angeben.



4. Wählen Sie Change.
5. Wählen Sie das Navigationsmenü-Symbol im oberen linken Bereich der WHM-Konsole.

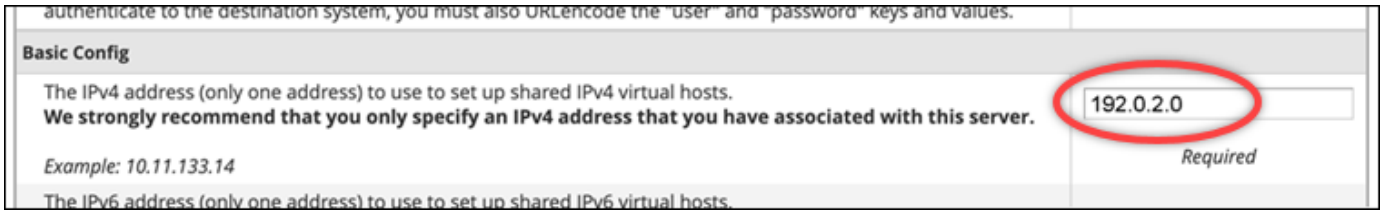


6. Wählen Sie Basic WebHost Manager Setup aus.



7. Scrollen Sie unter der Registerkarte Alle nach unten und suchen Sie den Abschnitt Basic Config der Seite.

8. Geben Sie im Textfeld der IPv4-Adresse die neue statische IP-Adresse der Instance ein. Weitere Informationen über IPv6 finden Sie unter Konfigurieren von IPv6 auf cPanel-Instances.



9. Scrollen Sie auf der Seite nach unten und wählen Sie Änderungen Speichern.

> **Note**
>
> Wenn Sie eine Ungültige Lizenzdatei-Fehlermeldung erhalten, warten Sie und versuchen Sie nach ein paar Minuten erneut, die IP-Adresse zu ändern.

Der Hostname und die IP-Adresse Ihrer Instance werden jetzt geändert, Sie müssen jedoch weiterhin Ihren Domainnamen Ihrer cPanel & WHM-Instance zuordnen. Fügen Sie dazu einen Adresseintrag (A) im Domain Name System (DNS) Ihres registrierten Domänennamen hinzu. Der A-Datensatz löst den Hostnamen Ihrer Instance in die statische IP-Adresse Ihrer Instance auf. Im nächsten Abschnitt in diesem Leitfaden zeigen wir Ihnen, wie Sie dabei vorgehen.

Schritt 5: Ordnen Sie Ihren Domänennamen Ihrer cPanel & WHM-Instance zu

> **Note**
>
> Sie können Ihrer cPanel & WHM-Instance eine Domain zuordnen, mit der Sie auf die WHM-Konsole zugreifen können. Sie können auch mehrere Domains innerhalb des WHM-Bereichs zuordnen, die Sie zur Verwaltung von Websites innerhalb des WHM-Bereichs verwenden können. In diesem Abschnitt wird beschrieben, wie Sie Ihre Domain Ihrer WHM-Instance zuordnen. Weitere Informationen zum Mapping mehrerer Domains in der WHM-Konsole, die Sie beim Erstellen eines neuen Kontos durchführen, finden Sie unter Neues Konto erstellen in der WHM-Dokumentation.

Um Ihren Domänennamen, wie z. B. `management.example.com`, auf Ihre `administration.example.com`-Instance abzubilden, fügen Sie einen Datensatz zum Domain Name System (DNS) Ihrer Domäne hinzu. Der Datensatz ordnet den Hostnamen Ihrer cPanel & WHM-Instance der statischen IP-Adresse Ihrer Instance zu. Die Unterdomäne, die Sie im A-Eintrag

angeben, muss mit dem Hostnamen übereinstimmen, den Sie im Abschnitt Schritt 4: Ändern des Hostnamens und der IP-Adresse Ihrer cPanel & WHM-Instance weiter oben in diesem Leitfaden angegeben haben. Nachdem der A-Eintrag hinzugefügt wurde, können Sie die folgende Adresse verwenden, um auf die WHM-Konsole Ihrer Instance zuzugreifen, anstatt die statische IP-Adresse Ihrer Instance zu verwenden. Ersetzen Sie *<InstanceHostName>* durch den Hostnamen Ihrer Instance.

```
https://<InstanceHostName>/whm
```

Beispiel:

```
https//management.example.com/whm
```

DNS-Datensätze werden in der Regel beim Registrar verwaltet und gehostet, bei dem Sie Ihre Domain registriert haben. Wir empfehlen jedoch, die Verwaltung der DNS-Datensätze Ihrer Domain auf Lightsail zu übertragen, damit Sie sie über die Lightsail-Konsole verwalten können. Melden Sie sich dazu bei der Lightsail-Konsole an. Wählen Sie auf der Startseite der Lightsail-Konsole die Registerkarte Domains und DNS und dann DNS-Zone erstellen aus. Folgen Sie den Anweisungen auf der Seite, um Ihren Domänennamen zu Lightsail hinzuzufügen. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain in Lightsail.

Schritt 6: Bearbeiten der Firewall Ihrer Instance

Die folgenden Firewall-Ports sind standardmäßig auf Ihrer cPanel & WHM-Instance geöffnet:

- SSH - TCP - 22
- DNS (UDP) - UDP - 53
- DNS (TCP) - TCP - 53
- HTTP - TCP - 80
- HTTPS - TCP - 443
- Benutzerdefiniert – TCP – 2078
- Benutzerdefiniert – TCP – 2083
- Benutzerdefiniert – TCP – 2087
- Benutzerdefiniert – TCP – 2089

Abhängig von den Diensten und Anwendungen, die Sie für Ihre Instance verwenden möchten, müssen Sie möglicherweise zusätzliche Ports öffnen. Öffnen Sie beispielsweise die Ports 25, 143, 465, 587, 993, 995, 2096 für E-Mail-Dienste und die Ports 2080, 2091 für Kalenderdienste. Wählen Sie auf der Registerkarte Networking (Netzwerk) auf Ihrer Instance-Verwaltungsseite unter dem Abschnitt Firewall die Option Add another (Weitere hinzufügen). Wählen Sie die zu öffnende Anwendung, das Protokoll und den Port oder den Portbereich aus. Wählen Sie anschließend Create.

Weitere Informationen darüber, welche Ports geöffnet werden sollen, finden Sie unter So konfigurieren Sie Ihre Firewall für cPanel-Dienste in der cPanel-Dokumentation. Weitere Informationen zum Bearbeiten der Firewall Ihrer Instance in Lightsail finden Sie unter Hinzufügen und Bearbeiten von Instance-Firewallregeln in Amazon Lightsail.

Schritt 7: Entfernen von SMTP-Einschränkungen aus Ihrer Lightsail-Instance

AWS blockiert ausgehenden Datenverkehr auf Port 25 auf allen Lightsail-Instances. Um ausgehenden Datenverkehr an Port 25 zu senden, beantragen Sie, dass diese Einschränkung entfernt wird. Weitere Informationen finden Sie unter Wie entferne ich die Einschränkung auf Port 25 von meiner Lightsail-Instance?.

> **Important**
>
> Wenn Sie SMTP für die Verwendung der Ports 25, 465 oder 587 konfigurieren, müssen Sie diese Ports in der Firewall Ihrer Instance in der Lightsail-Konsole öffnen. Weitere Informationen finden Sie unter Hinzufügen und Bearbeiten von Instance-Firewall-Regeln in Amazon Lightsail.

Schritt 8: Lesen Sie die cPanel & WHM-Dokumentation und erhalten Sie Unterstützung

Lesen Sie die cPanel & WHM-Dokumentation, um zu erfahren, wie Sie Websites mit cPanel und WHM verwalten. Weitere Informationen finden Sie unter cPanel & WHM-Dokumentation.

Wenn Sie Fragen zu cPanel & WHM haben oder Unterstützung benötigen, können Sie cPanel über die folgenden Ressourcen kontaktieren:

- Probleme bei Ihrer cPanel-Installation beheben
- cPanel-Discord channel

Schritt 9: Kauf einer Lizenz für cPanel & WHM

Ihre cPanel & WHM-Instance enthält eine 15-Tage-Testlizenz. Nach 15 Tagen müssen Sie eine Lizenz von cPanel erwerben, um weiterhin cPanel & WHM verwenden zu können. Weitere Informationen finden Sie unterWie kaufe ich eine cPanel-Lizenz?in der cPanel--Dokumentation.

> **Important**
>
> Sie müssen die öffentliche IP-Adresse Ihrer cPanel & WHM-Instance angeben, wenn Sie eine Lizenz von cPanel erwerben. Die Lizenz, die Sie kaufen, ist dieser IP-Adresse zugeordnet. Aus diesem Grund müssen Sie eine statische IP an Ihre cPanel & WHM-Instance anhängen, wie in Abschnitt Schritt 2: Anfügen einer statischen IP-Adresse an Ihre cPanel & WHM-Instance in diesem Leitfaden beschrieben. Geben Sie Ihre statische IP an, wenn Sie eine Lizenz von cPanel erwerben, und behalten Sie Ihre statische IP so lange bei, wie Sie Ihre cPanel & WHM-Lizenz mit einer Lightsail-Instance verwenden möchten. Wenn Sie Ihre Lizenz später an eine andere IP-Adresse übertragen müssen, können Sie eine Anfrage an cPanel senden. Weitere Informationen finden Sie unter Übertragen einer Lizenz in der WHM-Dokumentation.

Schritt 10: Erstellen eines Snapshots Ihrer cPanel & WHM-Instance

Ein Snapshot ist eine Kopie des Systemlaufwerks und der ursprünglichen Konfiguration einer Instance. Ein Snapshot enthält alle Daten, die erforderlich sind, um Ihre Instance wiederherzustellen (ab dem Zeitpunkt, an dem der Snapshot erstellt wurde). Sie können einen Snapshot als Grundlage für neue Instances oder als Datensicherung verwenden. Sie können jederzeit einen manuellen Snapshot erstellen oder automatische Snapshots aktivieren, damit Lightsail tägliche Snapshots für Sie erstellt.

> **Note**
>
> - Instance-Snapshots des Blueprints cPanel & WHM der aktuellen Generation für AlmaLinux können nach Amazon EC2 exportiert werden.
> - Instance-Snapshots der Vorlage cPanel und WHM der vorherigen Generation für AlmaLinux können nicht nach Amazon EC2 exportiert werden.

- Wenn Sie aus dem Snapshot eine neue Instance erstellen, geben Sie der Instance zusätzliche Zeit, um vollständig zu starten, bevor Sie sich beim WHM anmelden, wie in Schritt 3 beschrieben.

Geben Sie auf Ihrer Instance-Verwaltungsseite auf der Registerkarte Snapshot einen Namen für den Snapshot ein und wählen Sie dann Create snapshot (Snapshot erstellen) aus. Oder scrollen Sie zum Abschnitt Automatische Snapshots der Seite und wählen Sie den Schalter aus, um automatische Snapshots zu aktivieren.

Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Linux- oder Unix-Instance und Aktivieren oder Deaktivieren automatischer Snapshots für Instances oder Datenträger in Amazon Lightsail.

Schnellstart-Leitfaden: Drupal

Hier finden Sie einige erste Schritte, die Sie unternehmen sollten, nachdem Ihre Drupal-Instance auf Amazon Lightsail hochgefahren ist und läuft:

Inhalt

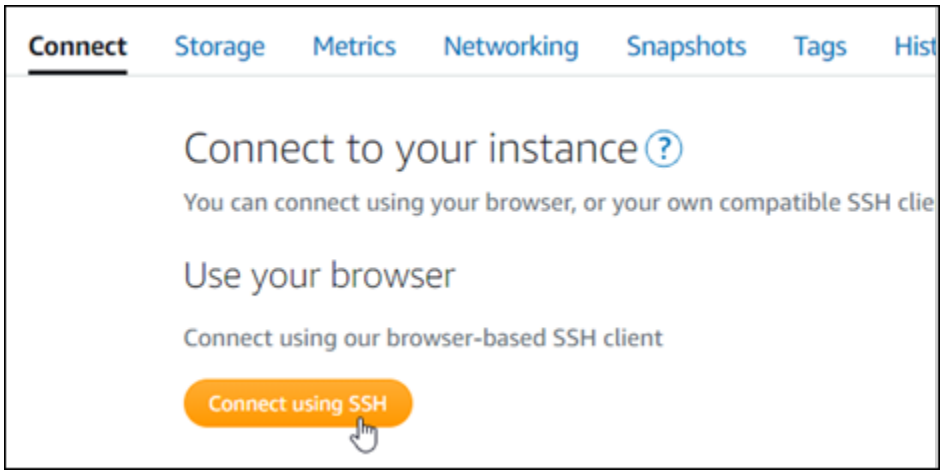
Schritt 1: Die Bitnami-Dokumentation lesen

Lesen Sie die Bitnami-Dokumentation, um zu erfahren, wie Sie Ihre Drupal-Anwendung konfigurieren. Weitere Informationen finden Sie unter Drupal-Paket von Bitnami für AWS Cloud.

Schritt 2: Das Standard-Anwendungspasswort für den Zugriff auf das Drupal-Verwaltungs-Dashboard einholen

Führen Sie das folgende Verfahren durch, um das Standard-Anwendungspasswort für den Zugriff auf das Verwaltungs-Dashboard für Ihre Drupal-Website zu erhalten. Weitere Informationen finden Sie unter Abrufen des Anwendungs-Benutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.

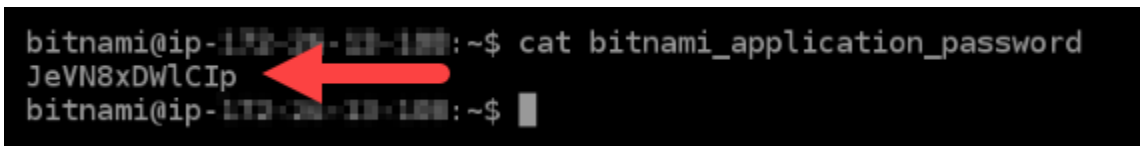
1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um das Anwendungspasswort zu erhalten:

```
cat $HOME/bitnami_application_password
```

Sie sollten eine ähnliche Antwort wie diese sehen, die das Standard-Anwendungspasswort enthält:



Schritt 3: Ihrer Instance eine statische IP-Adresse anfügen

Die Ihrer Instance beim ersten Erstellen zugewiesene öffentliche IP-Adresse ändert sich bei jedem Stopp und Start Ihrer Instance. Sie sollten eine statische IP-Adresse erstellen und an Ihre Instance anfügen, um sicherzustellen, dass sich deren öffentliche IP-Adresse nicht ändert. Wenn Sie Ihrer

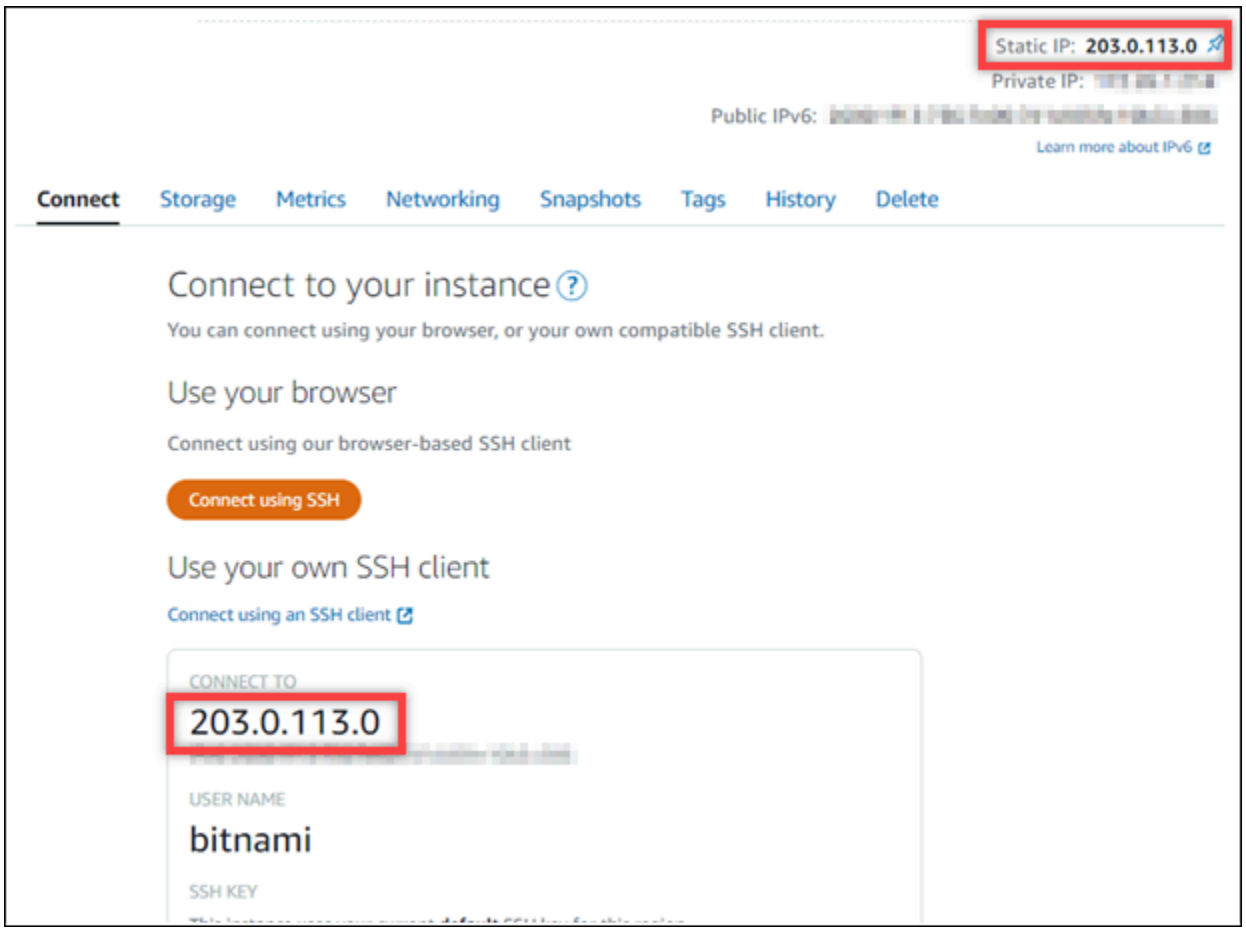
Instance später einen registrierten Domänennamen wie zum Beispiel `example.com` zuweisen, müssen Sie nicht jedes Mal, wenn Sie Ihre Instance stoppen und neu starten, die DNS-Akte Ihrer Domäne aktualisieren. Sie können eine statische IP an eine Instance anhängen.

Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Netzwerk, die Registerkarte Erstellen einer statischen IP oder Anfügen einer statischen IP (falls Sie zuvor eine statische IP-Adresse erstellt haben, die Sie Ihrer Instance anfügen können) und folgen Sie dann den Anweisungen auf der Seite. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

Schritt 4: Beim Verwaltungs-Dashboard für Ihre Drupal-Website anmelden

Nachdem Sie nun das Standard-Benutzerpasswort haben, navigieren Sie zur Startseite Ihrer Drupal-Website und melden Sie sich im Verwaltungs-Dashboard an. Nachdem Sie angemeldet sind, können Sie Ihre Website anpassen und administrative Änderungen vornehmen. Weitere Informationen zu den Möglichkeiten in Drupal finden Sie im Abschnitt Schritt 7: Die Drupal-Dokumentation lesen und Ihre Website weiter konfigurieren weiter unten in diesem Leitfaden.

1. Notieren Sie sich von Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die öffentliche IP-Adresse Ihrer Instance. Die öffentliche IP-Adresse wird auch im Kopfzeilenabschnitt Ihrer Instance-Verwaltungsseite angezeigt.



2. Navigieren Sie zur öffentlichen IP-Adresse ihrer Instance, indem Sie z B. zu `http://203.0.113.0` gehen.

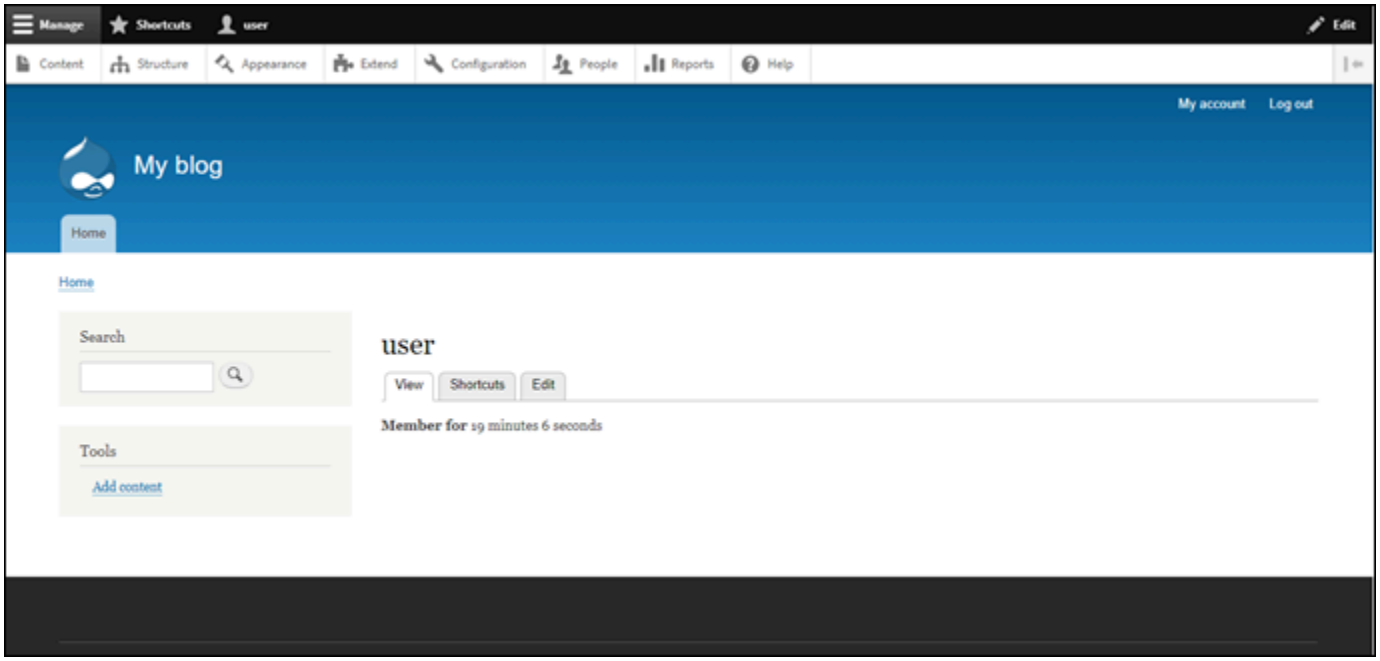
   Die Startseite Ihrer Drupal-Website sollte erscheinen.

3. Wählen Sie Manage (Verwalten) in der unteren rechten Ecke Ihrer Startseite der Drupal-Website.

   Wenn das Banner Manage (Verwalten) nicht angezeigt wird, können Sie die Anmeldeseite erreichen, indem Sie zu `http://<PublicIP>/user/login` gehen. Ersetzen Sie *`<PublicIP>`* durch die öffentliche IP-Adresse Ihrer Instance.

4. Melden Sie sich mit dem Standardbenutzernamen (`user`) und dem zuvor abgerufenen Standardpasswort an, wie vorhin in diesem Leitfaden beschrieben.

   Das Drupal-Verwaltungs-Dashboard wird angezeigt.



Schritt 5: Datenverkehr für Ihren registrierten Domänennamen auf Ihre Drupal-Website weiterleiten

Um den Datenverkehr für Ihren registrierten Domänennamen, z. B. `example.com`, auf Ihre Drupal-Website weiterzuleiten, fügen Sie zum Domain Name System (DNS) Ihrer Domain einen Datensatz hinzu. DNS-Datensätze werden in der Regel beim Registrar verwaltet und gehostet, bei dem Sie Ihre Domäne registriert haben. Wir empfehlen jedoch, die Verwaltung der DNS-Datensätze Ihrer Domäne auf Lightsail zu übertragen, damit Sie sie über die Lightsail-Konsole verwalten können.

Wählen Sie auf der Startseite der Lightsail-Konsole unter der Registerkarte Domains & DNS (Domains und DNS) die Option Create DNS zone (DNS-Zone erstellen) und folgen Sie dann den Anweisungen auf der Seite. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain in Lightsail.

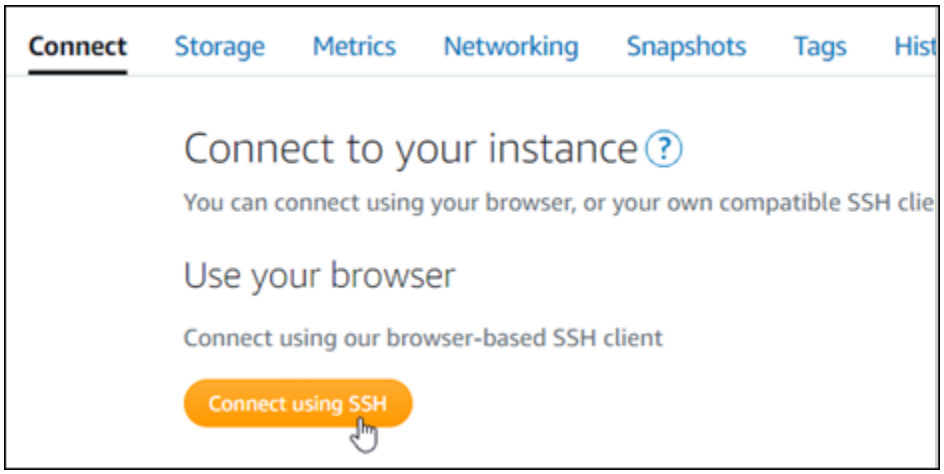
Wenn Sie zu dem Domänennamen navigieren, den Sie für Ihre Instance konfiguriert haben, sollten Sie zur Startseite Ihrer Drupal-Website umgeleitet werden. Als Nächstes sollten Sie ein SSL/TLS-Zertifikat erstellen und konfigurieren, um HTTPS-Verbindungen für Ihre Drupal-Website zu ermöglichen. Für weitere Informationen fahren Sie mit dem nächsten Abschnitt Schritt 6: HTTPS für Ihre Drupal-Website konfigurieren in diesem Leitfaden fort.

Schritt 6: HTTPS für Ihre Drupal-Website konfigurieren

Führen Sie die folgenden Schritte aus, um HTTPS auf Ihrer Drupal-Website zu konfigurieren. Diese Schritte zeigen Ihnen, wie Sie das Bitnami-HTTPS-Konfigurations-Tool (`bncert-tool`) verwenden, ein Befehlszeilentool zum Anfordern von SSL/TLS-Zertifikaten von Let's Encrypt. Weitere Informationen finden Sie unter Erfahren Sie mehr über das Bitnami-HTTPS-Konfigurations-Tool in der Bitnami-Dokumentation.

> **Important**
>
> Bevor Sie mit diesem Verfahren beginnen, stellen Sie sicher, dass Sie Ihre Domäne so konfiguriert haben, dass der Datenverkehr an Ihre Drupal-Instance weitergeleitet wird. Andernfalls schlägt die SSL/TLS-Zertifikatvalidierung fehl.

1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um zu bestätigen, dass das bncert-Tool auf Ihrer Instance installiert ist.

```
sudo /opt/bitnami/bncert-tool
```

   Sie sollten eine der folgenden Antworten sehen:

   - Wenn Sie den Befehl in der Antwort nicht gefunden haben, ist das bncert-Tool auf Ihrer Instance nicht installiert. Fahren Sie mit dem nächsten Schritt in diesem Verfahren fort, um das bncert-Tool auf Ihrer Instance zu installieren.

- Wenn in der Antwort Willkommen beim HTTPS-Konfigurationstool von Bitnami angezeigt wird, ist das bncert-Tool auf Ihrer Instance installiert. Fahren Sie mit Schritt 8 dieses Verfahrens fort.
- Wenn das bncert-Tool bereits eine Zeit lang auf Ihrer Instance installiert ist, wird möglicherweise eine Meldung angezeigt, die angibt, dass eine aktualisierte Version des Tools verfügbar ist. Wählen Sie, es herunterzuladen, und geben Sie dann den `sudo /opt/bitnami/bncert-tool`-Befehl ein, um das bncert-Tool erneut auszuführen. Fahren Sie mit Schritt 8 dieses Verfahrens fort.

3. Geben Sie den folgenden Befehl ein, um die bncert-Laufdatei auf Ihre Instance herunterzuladen.

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. Geben Sie den folgenden Befehl ein, um ein Verzeichnis für die bncert-Tool-Laufdatei auf Ihrer Instance zu erstellen.

```
sudo mkdir /opt/bitnami/bncert
```

5. Geben Sie den folgenden Befehl ein, um die bncrt-Laufdatei als ein Programm auszuführen.

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. Geben Sie den folgenden Befehl ein, um einen symbolischen Link zu erstellen, der das bncert-Tool ausführt, wenn Sie den Befehl sudo /opt/bitnami/bncert-tool eingeben.

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

   Sie sind jetzt fertig mit der Installation des bncert-Tools auf Ihrer Instance.

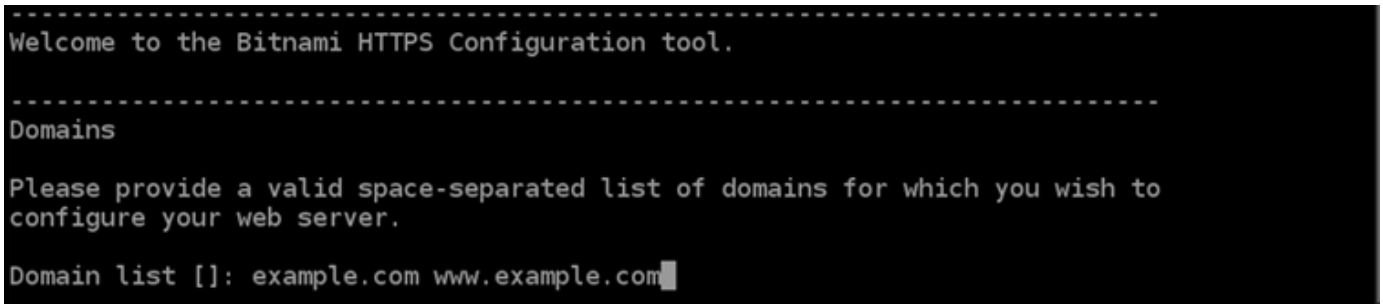
7. Geben Sie den folgenden Befehl ein, um das bncert-Tool auszuführen.

```
sudo /opt/bitnami/bncert-tool
```

8. Geben Sie Ihren primären Domänennamen und alternative Domänennamen durch ein Leerzeichen getrennt ein, wie im folgenden Beispiel gezeigt.

   Wenn Ihre Domäne nicht darauf konfiguriert ist, Datenverkehr auf die öffentliche IP-Adresse Ihrer Instance umzuleitent, wird das`bncert`-Tool Sie aufgefordern, diese Konfiguration vorzunehmen, bevor Sie fortfahren. Ihre Domäne muss den Datenverkehr an die öffentliche IP-Adresse der Instance weiterleiten, von der Sie das `bncert`-Tool verwenden, um HTTPS für die Instance zu

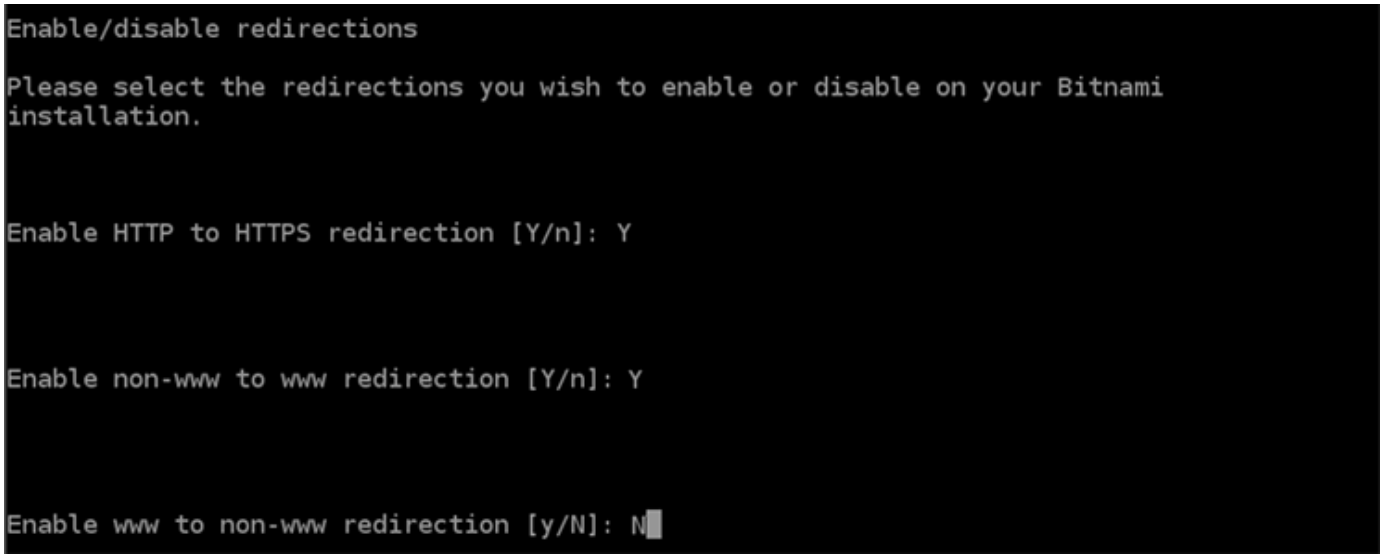
aktivieren. Dies bestätigt, dass Sie Eigentümer der Domäne sind und dient als Validierung für Ihr Zertifikat.



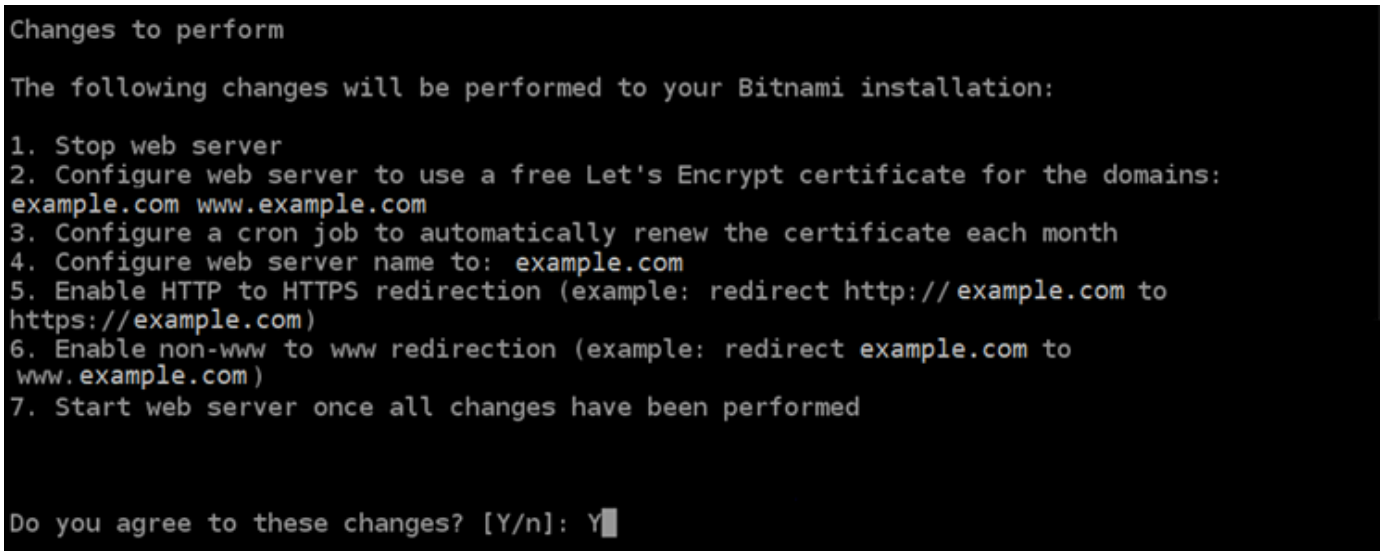
9. Das `bncert`-Tool wird Sie fragen, wie die Umleitung Ihrer Website konfiguriert werden soll. Die folgenden Optionen sind verfügbar:

   - Aktivieren einer Umleitung von HTTP zu HTTPS- Gibt an, ob Benutzer, die zur HTTP-Version Ihrer Website navigieren (d. h.`http:/example.com`) automatisch auf die HTTPS-Version umgeleitet (d.h.`https://example.com`) werden. Wir empfehlen, diese Option zu aktivieren, da sie alle Besucher zwingt, die verschlüsselte Verbindung zu verwenden. `Y` eingeben und Eingabe drücken, um dies zu aktivieren.
   - Umleitung von Nicht-www zu www aktivieren- Gibt an, ob Benutzer, die zur Spitze Ihrer Domäne navigieren (d. h.`https://example.com`) automatisch an die`www`Unterdomäne Ihrer Domäne (d. h.`https://www.example.com`) weitergeleitet werden. Wir empfehlen, diese Option zu auszuwählen. Sie können diese jedoch deaktivieren und die alternative Option aktivieren (aktivieren Sie`www` auf Nicht-`www` Umleiten), wenn Sie die Spitze Ihrer Domäne als bevorzugte Website-Adresse in Suchmaschinentools wie den Webmaster-Tools von Google angegeben haben, oder wenn Ihre Spitze direkt auf Ihre IP verweist und Ihre `www` Unterdomäne Ihren Apex über eine CNAME-Akte referenziert. `Y` eingeben und Eingabe drücken, um dies zu aktivieren.
   - Umleitung von Nicht-www zu www aktivieren- Gibt an, ob Benutzer, die zur Unterdomäne Ihrer Domäne `www` navigieren (d. h.`https://www.example.com`) automatisch an die Spitze Ihrer Domäne (d. h.`https://example.com`) weitergeleitet werden. Wir empfehlen dies zu deaktivieren, wenn Sie Nicht-`www`Umleiten auf`www` aktiviert haben. `N` eingeben und Eingabe drücken, um dies zu aktivieren.

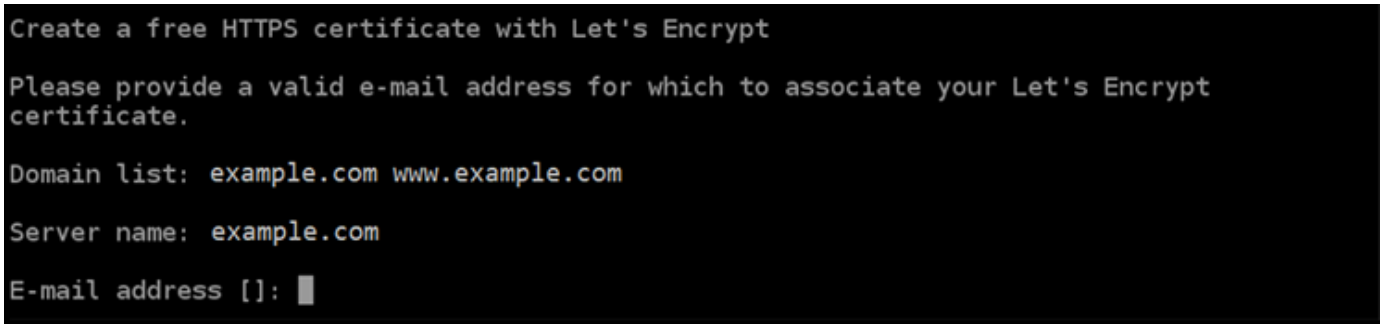
   Ihre Auswahl sollte wie im folgenden Beispiel aussehen.



10. Die Änderungen, die vorgenommen werden, sind aufgelistet. Y eingeben undEingabe drücken, um zu bestätigen und fortzufahren.



11. Geben Sie Ihre E-Mail-Adresse ein, die Sie Ihrem Let's-Encrypt-Zertifikat zuordnen möchten, und drücken SieEingabe.



12. Lesen Sie die Let's-Encrypt-Subscriber-Vereinbarung. Y eingeben undEingabe drücken, um die Vereinbarung zu akzeptieren und fortzufahren.

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

Die Aktionen werden ausgeführt, um HTTPS für Ihre Instance zu aktivieren, einschließlich der Anforderung des Zertifikats und der Konfiguration der angegebenen Umleitungen.

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.
```

Ihr Zertifikat wurde erfolgreich ausgestellt und validiert, und die Umleitungen werden erfolgreich für Ihre Instance konfiguriert, wenn eine Meldung ähnlich dem folgenden Beispiel angezeigt wird.

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:
```

Das `bncert`-Tool führt alle 80 Tage vor Ablauf Ihres Zertifikats eine automatische Erneuerung durch. Wiederholen Sie die obigen Schritte, wenn Sie zusätzliche Domänen und Unterdomänen mit Ihrer Instance verwenden möchten und Sie HTTPS für diese Domänen aktivieren möchten.

Sie sind jetzt fertig, HTTPS auf Ihrer Drupal-Instance zu aktivieren. Wenn Sie das nächste Mal mit der von Ihnen konfigurierten Domäne zu Ihrer Drupal-Website navigieren, sollten Sie sehen, dass sie auf die HTTPS-Verbindung umgeleitet wird.

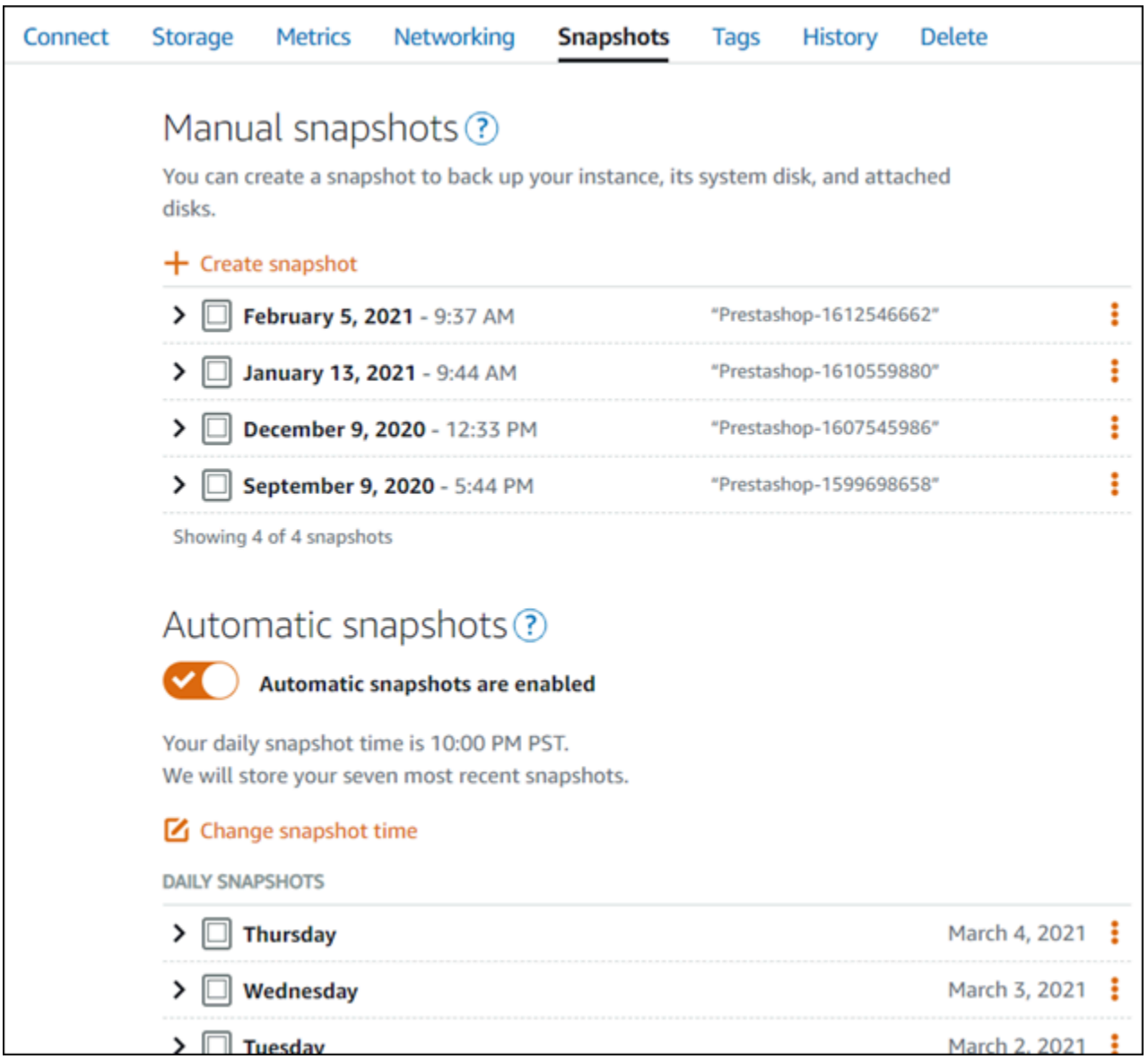
Schritt 7: Die Drupal-Dokumentation lesen und Ihre Website weiter konfigurieren

Lesen Sie die Drupal-Dokumentation, um zu erfahren, wie Sie Ihre Website verwalten und anpassen. Weitere Informationen finden Sie in der Drupal-Dokumentation.

Schritt 8: Einen Snapshot Ihrer Instance erstellen

Nachdem Sie Ihre Drupal-Website so konfiguriert haben, wie Sie sie möchten, erstellen Sie periodische Snapshots Ihrer Instance, um diese zu sichern. Sie können Snapshots manuell erstellen oder automatische Snapshots aktivieren, damit Lightsail tägliche Snapshots für Sie erstellt.. Wenn etwas mit Ihrer Instance nicht stimmt, können Sie mit dem Snapshot eine neue Ersatz-Instance erstellen. Weitere Informationen finden Sie unter Snapshots.

Wählen Sie auf der Instance-Verwaltungsseite, unter der RegisterkarteSnapshotSnapshot erstellenoder wählen Sie aus, automatische Snapshots zu aktivieren.



Weitere Informationen finden Sie unter Erstellen eines Snapshots IhrerLinux- oder Unix-Instance inAmazon LightsailoderAktivieren oder Deaktivieren von automatischen Snapshots für Instances oder Datenträger inAmazon Lightsail.

Schnellstartanleitung: Ghost

Hier finden Sie einige erste Schritte, die Sie unternehmen sollten, nachdem Ihre Ghost-Instance auf Amazon Lightsail hochgefahren ist und läuft:

Inhalt

- Schritt 2: Das Standard-Anwendungspasswort für den Zugriff auf das Ghost-Verwaltungs-Dashboard einholen
- Schritt 3: Ihrer Instance eine statische IP-Adresse anfügen
- Schritt 4: Beim Verwaltungs-Dashboard für Ihre Ghost-Website anmelden
- Schritt 5: Datenverkehr für Ihren registrierten Domänennamen auf Ihre Ghost-Website weiterleiten
- Schritt 6: HTTPS für Ihre Ghost-Website konfigurieren
- Schritt 7: Die Ghost-Dokumentation lesen und Ihre Website weiter konfigurieren
- Schritt 8: Einen Snapshot Ihrer Instance erstellen

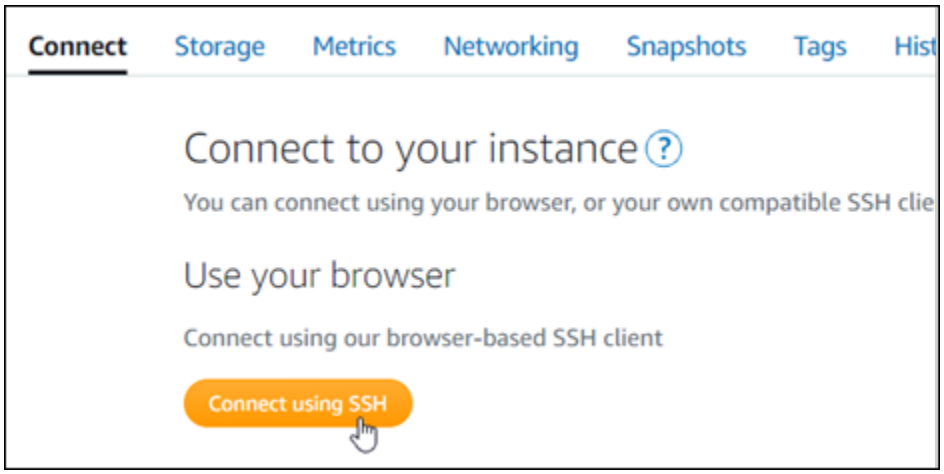
Schritt 1: Die Bitnami-Dokumentation lesen

Lesen Sie die Bitnami-Dokumentation, um zu erfahren, wie Sie Ihre Ghost-Anwendung konfigurieren. Weitere Informationen finden Sie unter Ghost von Bitnami für die AWS Cloud verpackt.

Schritt 2: Das Standard-Anwendungspasswort für den Zugriff auf das Ghost-Verwaltungs-Dashboard einholen

Führen Sie das folgende Verfahren durch, um das Standard-Anwendungspasswort für den Zugriff auf das Verwaltungs-Dashboard für Ihre Ghost-Website zu erhalten. Weitere Informationen finden Sie unter Abrufen des Anwendungs-Benutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.

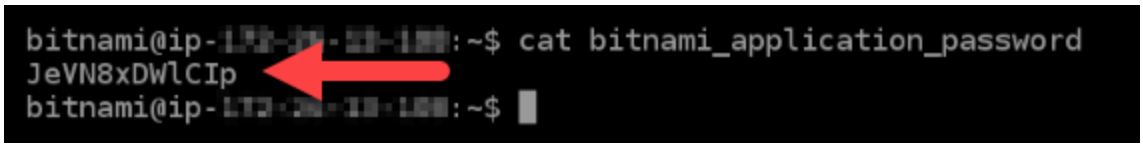
1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um das Anwendungspasswort zu erhalten:

```
cat $HOME/bitnami_application_password
```

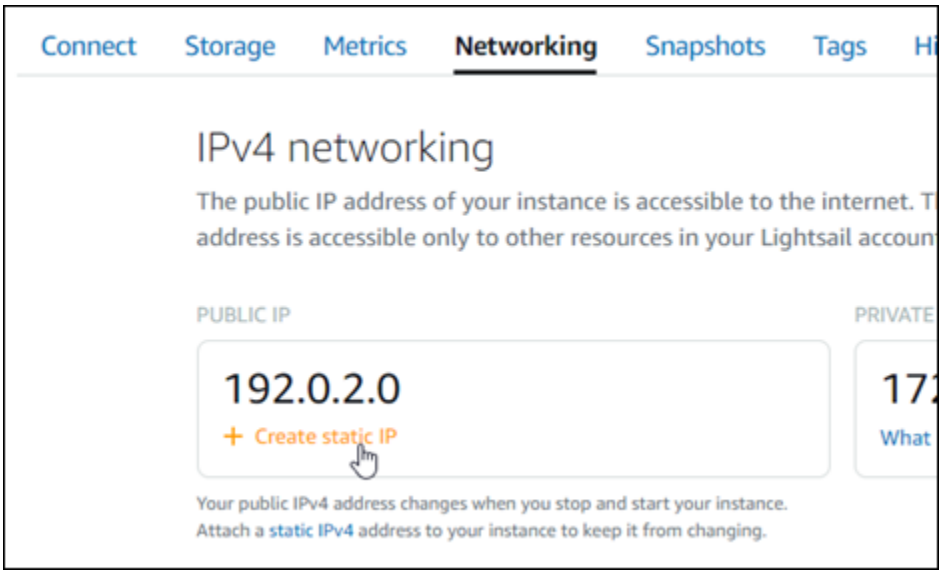
Sie sollten eine ähnliche Antwort wie diese sehen, die das Standard-Anwendungspasswort enthält:



Schritt 3: Ihrer Instance eine statische IP-Adresse anfügen

Die Ihrer Instance beim ersten Erstellen zugewiesene öffentliche IP-Adresse ändert sich bei jedem Stopp und Start Ihrer Instance. Sie sollten eine statische IP-Adresse erstellen und an Ihre Instance anfügen, um sicherzustellen, dass sich deren öffentliche IP-Adresse nicht ändert. Wenn Sie Ihrer Instance später einen registrierten Domänennamen wie zum Beispiel `example.com` zuweisen, müssen Sie nicht jedes Mal, wenn Sie Ihre Instance stoppen und neu starten, die DNS-Akte Ihrer Domäne aktualisieren. Sie können eine statische IP an eine Instance anhängen.

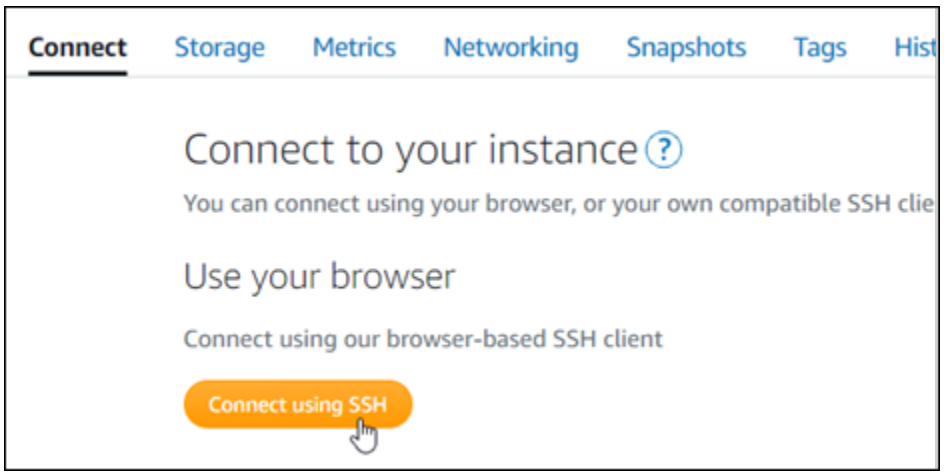
Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Netzwerk, die Registerkarte Erstellen einer statischen IP oder Anfügen einer statischen IP (falls Sie zuvor eine statische IP-Adresse erstellt haben, die Sie Ihrer Instance anfügen können) und folgen Sie dann den Anweisungen auf der Seite. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.



Nachdem die neue statische IP-Adresse an Ihre Instance angefügt wurde, müssen Sie die folgenden Schritte ausführen, um die Anwendung auf die neue statische IP-Adresse aufmerksam zu machen.

1. Notieren Sie sich die statische IP-Adresse Ihrer Instance. Sie wird im Kopfzeilenabschnitt Ihrer Instance-Verwaltungsseite aufgeführt.

2. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Verbinden die Option Verbinden mit SSH.



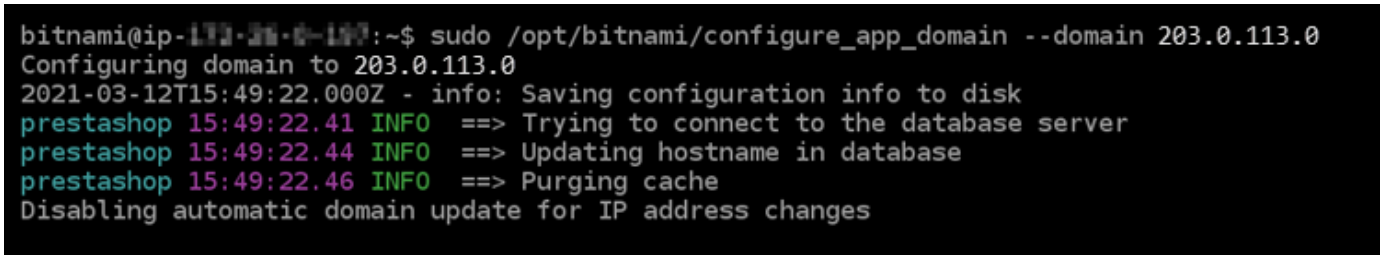
3. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein. Stellen Sie sicher, dass Sie *<StaticIP>* mit der neuen statischen IP-Adresse Ihrer Instance ersetzen.

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

Beispiel:

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

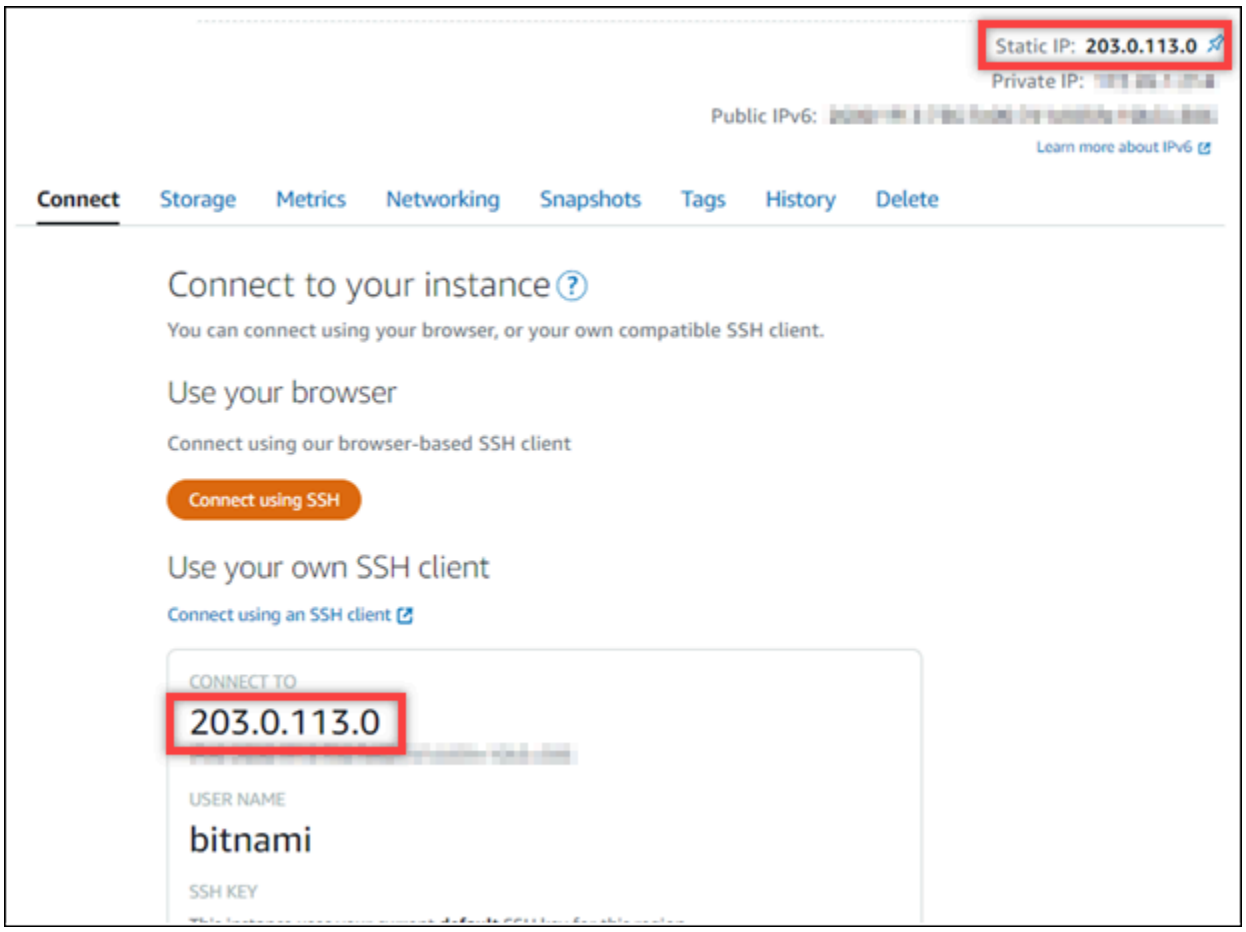
Sie sollten eine Reaktion ähnlich dem folgenden Beispiel erhalten. Die Anwendung auf Ihrer Instance sollte nun die neue statische IP-Adresse erkannt haben.



Schritt 4: Anmeldung beim Verwaltungs-Dashboard für Ihre Ghost-Website

Nachdem Sie nun das Standard-Anwendungspasswort haben, führen Sie das folgende Verfahren aus, um zur Startseite Ihrer Ghost-Website zu navigieren und sich beim Verwaltungs-Dashboard anzumelden. Nachdem Sie angemeldet sind, können Sie Ihre Website anpassen und administrative Änderungen vornehmen. Weitere Informationen zu den Möglichkeiten in Ghost finden Sie im Abschnitt Schritt 6: Die Ghost-Dokumentation lesen und Ihre Website weiter konfigurieren weiter unten in diesem Leitfaden.

1. Notieren Sie sich von Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die öffentliche IP-Adresse Ihrer Instance. Die öffentliche IP-Adresse wird auch im Kopfzeilenabschnitt Ihrer Instance-Verwaltungsseite angezeigt.



2. Navigieren Sie zur öffentlichen IP-Adresse ihrer Instance, indem Sie z B. zu `http://203.0.113.0` gehen.

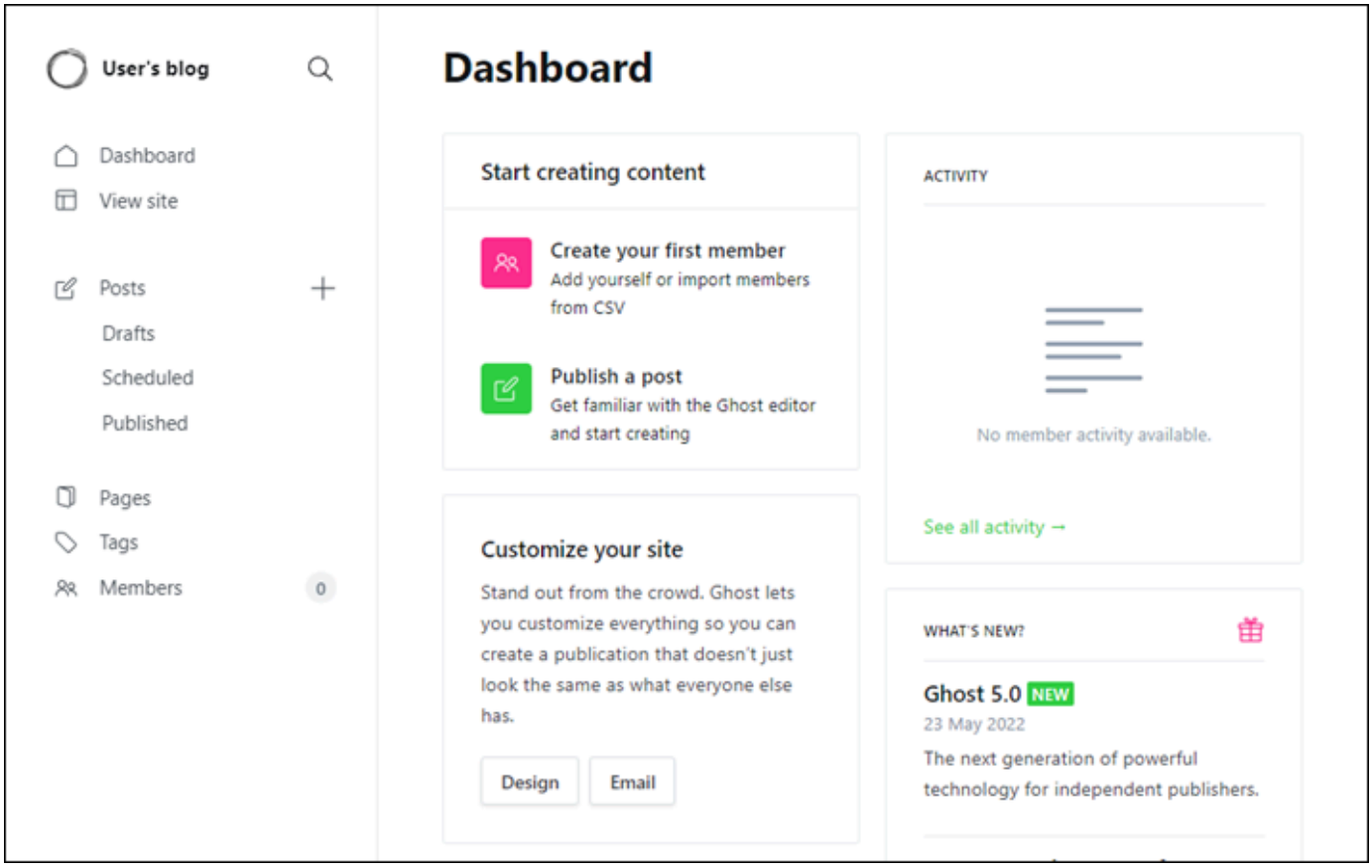
   Die Startseite Ihrer Ghost-Website sollte erscheinen.

3. Wählen Sie Manage (Verwalten) in der unteren rechten Ecke Ihrer Startseite der Ghost-Website.

   Wenn das Banner Manage (Verwalten) nicht angezeigt wird, können Sie die Anmeldeseite erreichen, indem Sie zu `http://<PublicIP>/ghost` gehen. Ersetzen Sie *<PublicIP>* durch die öffentliche IP-Adresse Ihrer Instance.

4. Melden Sie sich mit dem Standardbenutzernamen (`user@example.com`) und dem zuvor abgerufenen Standardpasswort an, wie vorhin in diesem Leitfaden beschrieben.

   Das Ghost-Verwaltungs-Dashboard wird angezeigt.



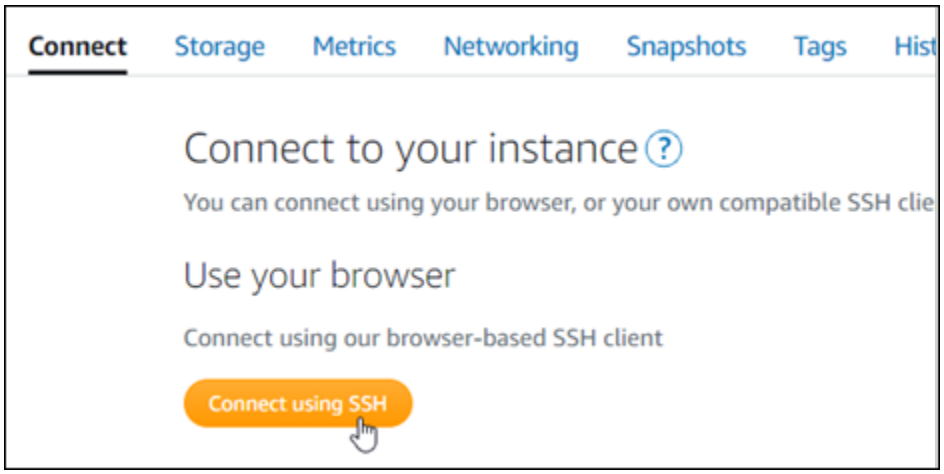
Schritt 5: Datenverkehr für Ihren registrierten Domänennamen auf Ihre Ghost-Website weiterleiten

Um den Datenverkehr für Ihren registrierten Domainnamen, z. B. `example.com`, auf Ihrer Ghost-Website weiterzuleiten, fügen Sie zum DNS Ihrer Domain einen Datensatz hinzu. DNS-Datensätze werden in der Regel beim Registrar verwaltet und gehostet, bei dem Sie Ihre Domäne registriert haben. Wir empfehlen jedoch, die Verwaltung der DNS-Datensätze Ihrer Domäne auf Lightsail zu übertragen, damit Sie sie über die Lightsail-Konsole verwalten können.

Wählen Sie auf der Startseite der Lightsail-Konsole unter der Registerkarte Domains & DNS (Domains und DNS) die Option Create DNS zone (DNS-Zone erstellen) und folgen Sie dann den Anweisungen auf der Seite. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain in Lightsail.

Nachdem Ihr Domänenname Datenverkehr an Ihre Instance weitergeleitet hat, müssen Sie die folgenden Schritte ausführen, um die Ghost-Software auf den Domänennamen aufmerksam zu machen.

1. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Verbinden die Option Verbinden mit SSH.



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein. Stellen Sie sicher, dass Sie *<DomainName>* mit dem Domänennamen ersetzen, der Datenverkehr an Ihre Ghost-Instance weiterleitet.

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

   Beispiel:

```
sudo /opt/bitnami/configure_app_domain --domain example.com
```

   Sie sollten eine Reaktion ähnlich dem folgenden Beispiel erhalten. Die Ghost-Anwendung sollte nun die Domäne erkannt haben.

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain example.com
Configuring domain to example.com
2022-06-09T22:25:58.177Z - info: Saving configuration info to disk
ghost 22:25:58.57 INFO  ==> Configuring Ghost URL to http://example.com
Disabling automatic domain update for IP address changes
```

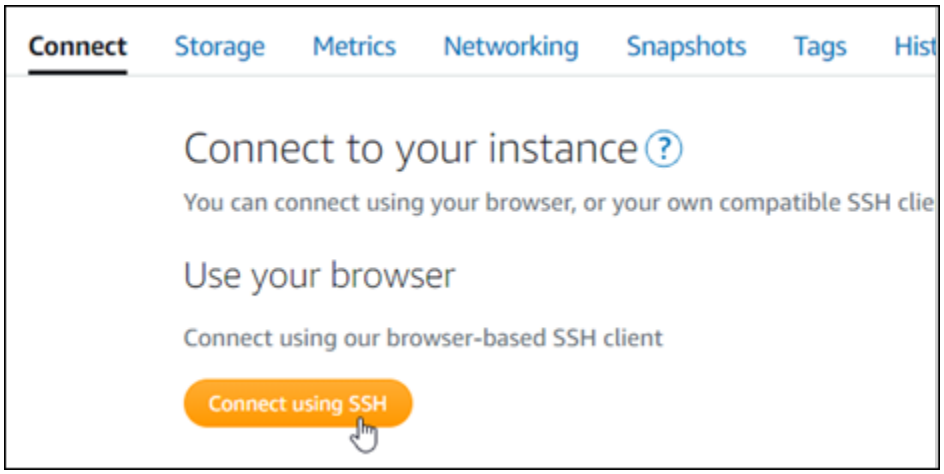
Wenn Sie zu dem Domänennamen navigieren, den Sie für Ihre Instance konfiguriert haben, sollten Sie zur Startseite Ihrer Ghost-Website umgeleitet werden. Als Nächstes sollten Sie ein SSL/TLS-Zertifikat erstellen und konfigurieren, um HTTPS-Verbindungen für Ihre Ghost-Website zu ermöglichen. Für weitere Informationen fahren Sie mit dem nächsten Abschnitt Schritt 6: HTTPS für Ihre Ghost-Website konfigurieren in diesem Leitfaden fort.

Schritt 6: HTTPS für Ihre Ghost-Website konfigurieren

Führen Sie die folgenden Schritte aus, um HTTPS auf Ihrer Ghost-Website zu konfigurieren. Diese Schritte zeigen Ihnen, wie Sie das Bitnami-HTTPS-Konfigurations-Tool (`bncert-tool`) verwenden, ein Befehlszeilentool zum Anfordern von SSL/TLS-Zertifikaten von Let's Encrypt. Weitere Informationen finden Sie unter Erfahren Sie mehr über das Bitnami-HTTPS-Konfigurations-Tool in der Bitnami-Dokumentation.

> **Important**
>
> Bevor Sie mit diesem Verfahren beginnen, stellen Sie sicher, dass Sie Ihre Domäne so konfiguriert haben, dass der Datenverkehr an Ihre Ghost-Instance weitergeleitet wird. Andernfalls schlägt die SSL/TLS-Zertifikatvalidierung fehl.

1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um zu bestätigen, dass das bncert-Tool auf Ihrer Instance installiert ist.

```
sudo /opt/bitnami/bncert-tool
```

   Sie sollten eine der folgenden Antworten sehen:

   - Wenn Sie den Befehl in der Antwort nicht gefunden haben, ist das bncert-Tool auf Ihrer Instance nicht installiert. Fahren Sie mit dem nächsten Schritt in diesem Verfahren fort, um das bncert-Tool auf Ihrer Instance zu installieren.

- Wenn in der Antwort Willkommen beim HTTPS-Konfigurationstool von Bitnami angezeigt wird, ist das bncert-Tool auf Ihrer Instance installiert. Fahren Sie mit Schritt 8 dieses Verfahrens fort.
- Wenn das bncert-Tool bereits eine Zeit lang auf Ihrer Instance installiert ist, wird möglicherweise eine Meldung angezeigt, die angibt, dass eine aktualisierte Version des Tools verfügbar ist. Wählen Sie, es herunterzuladen, und geben Sie dann den `sudo /opt/bitnami/bncert-tool`-Befehl ein, um das bncert-Tool erneut auszuführen. Fahren Sie mit Schritt 8 dieses Verfahrens fort.

3. Geben Sie den folgenden Befehl ein, um die bncert-Laufdatei auf Ihre Instance herunterzuladen.

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. Geben Sie den folgenden Befehl ein, um ein Verzeichnis für die bncert-Tool-Laufdatei auf Ihrer Instance zu erstellen.

```
sudo mkdir /opt/bitnami/bncert
```

5. Geben Sie den folgenden Befehl ein, um die bncrt-Laufdatei als ein Programm auszuführen.

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. Geben Sie den folgenden Befehl ein, um einen symbolischen Link zu erstellen, der das bncert-Tool ausführt, wenn Sie den Befehl sudo /opt/bitnami/bncert-tool eingeben.

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

   Sie sind jetzt fertig mit der Installation des bncert-Tools auf Ihrer Instance.

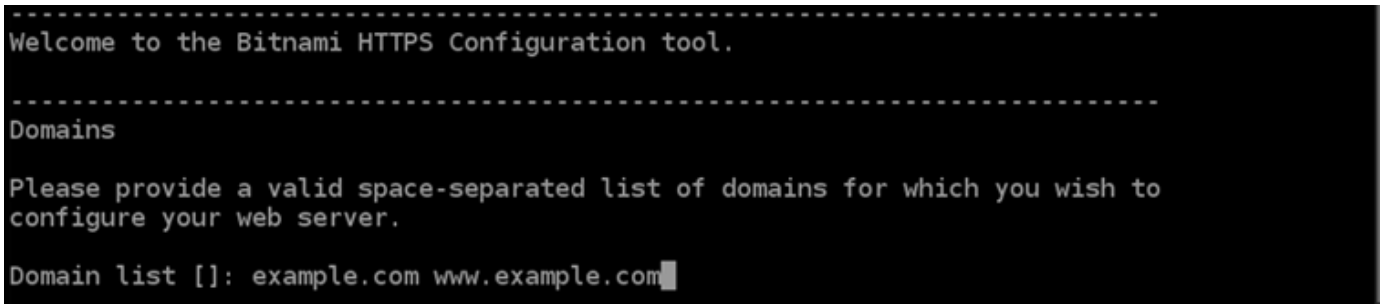
7. Geben Sie den folgenden Befehl ein, um das bncert-Tool auszuführen.

```
sudo /opt/bitnami/bncert-tool
```

8. Geben Sie Ihren primären Domänennamen und alternative Domänennamen durch ein Leerzeichen getrennt ein, wie im folgenden Beispiel gezeigt.

   Wenn Ihre Domäne nicht darauf konfiguriert ist, Datenverkehr auf die öffentliche IP-Adresse Ihrer Instance umzuleitent, wird das`bncert`-Tool Sie aufgefordern, diese Konfiguration vorzunehmen, bevor Sie fortfahren. Ihre Domäne muss den Datenverkehr an die öffentliche IP-Adresse der Instance weiterleiten, von der Sie das `bncert`-Tool verwenden, um HTTPS für die Instance zu

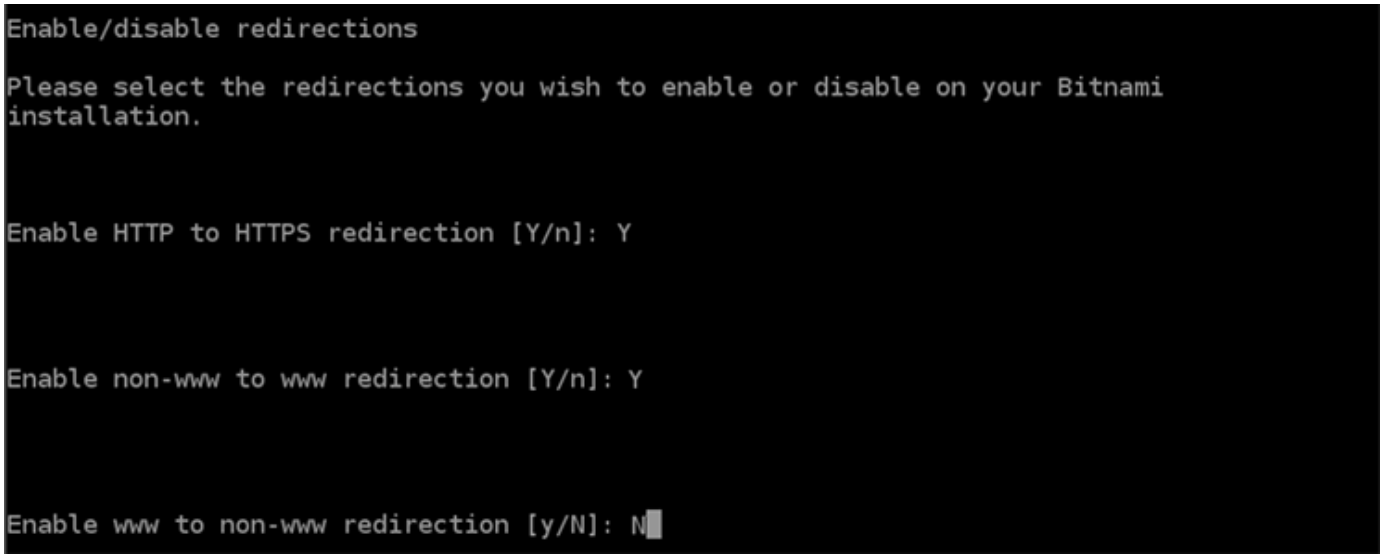
aktivieren. Dies bestätigt, dass Sie Eigentümer der Domäne sind und dient als Validierung für Ihr Zertifikat.



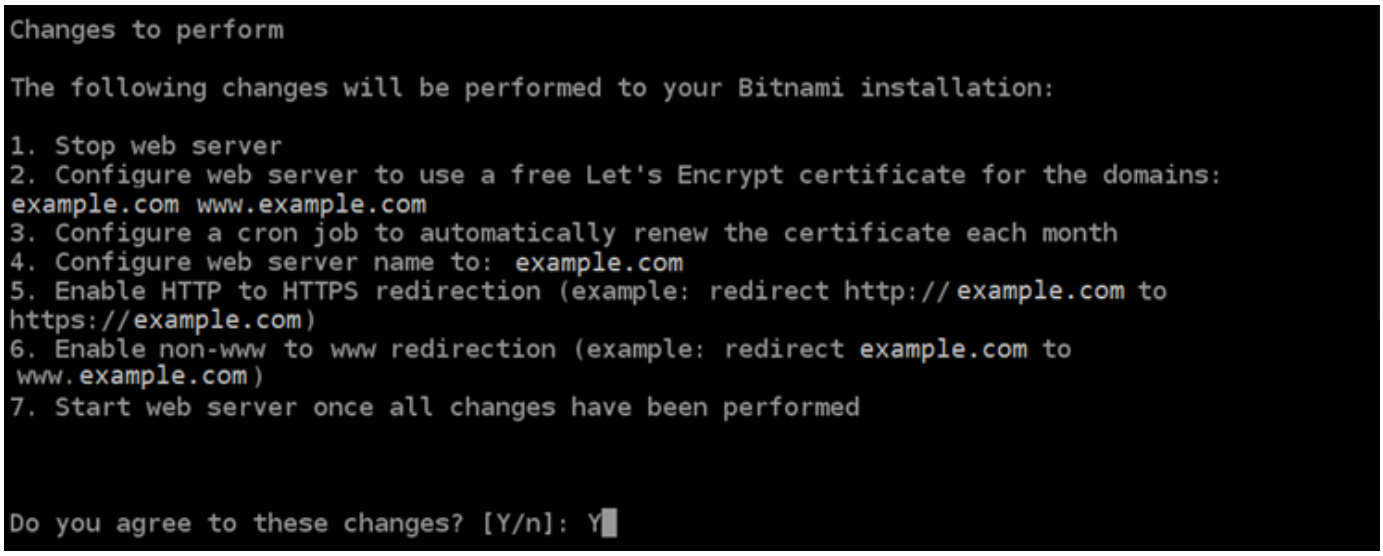
9. Das `bncert`-Tool wird Sie fragen, wie die Umleitung Ihrer Website konfiguriert werden soll. Die folgenden Optionen sind verfügbar:

   - Aktivieren einer Umleitung von HTTP zu HTTPS- Gibt an, ob Benutzer, die zur HTTP-Version Ihrer Website navigieren (d. h.`http:/example.com`) automatisch auf die HTTPS-Version umgeleitet (d.h.`https://example.com`) werden. Wir empfehlen, diese Option zu aktivieren, da sie alle Besucher zwingt, die verschlüsselte Verbindung zu verwenden. `Y` eingeben und Eingabe drücken, um dies zu aktivieren.
   - Umleitung von Nicht-www zu www aktivieren- Gibt an, ob Benutzer, die zur Spitze Ihrer Domäne navigieren (d. h.`https://example.com`) automatisch an die`www`Unterdomäne Ihrer Domäne (d. h.`https://www.example.com`) weitergeleitet werden. Wir empfehlen, diese Option zu auszuwählen. Sie können diese jedoch deaktivieren und die alternative Option aktivieren (aktivieren Sie`www` auf Nicht-`www` Umleiten), wenn Sie die Spitze Ihrer Domäne als bevorzugte Website-Adresse in Suchmaschinentools wie den Webmaster-Tools von Google angegeben haben, oder wenn Ihre Spitze direkt auf Ihre IP verweist und Ihre `www` Unterdomäne Ihren Apex über eine CNAME-Akte referenziert. `Y` eingeben und Eingabe drücken, um dies zu aktivieren.
   - Umleitung von Nicht-www zu www aktivieren- Gibt an, ob Benutzer, die zur Unterdomäne Ihrer Domäne `www` navigieren (d. h.`https://www.example.com`) automatisch an die Spitze Ihrer Domäne (d. h.`https://example.com`) weitergeleitet werden. Wir empfehlen dies zu deaktivieren, wenn Sie Nicht-`www`Umleiten auf`www` aktiviert haben. `N` eingeben und Eingabe drücken, um dies zu aktivieren.

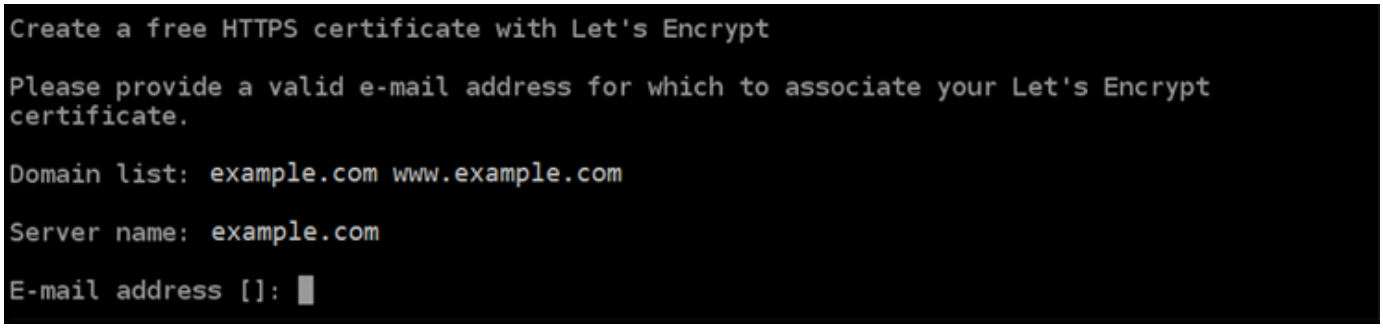
   Ihre Auswahl sollte wie im folgenden Beispiel aussehen.



10. Die Änderungen, die vorgenommen werden, sind aufgelistet. Y eingeben undEingabe drücken, um zu bestätigen und fortzufahren.



11. Geben Sie Ihre E-Mail-Adresse ein, die Sie Ihrem Let's-Encrypt-Zertifikat zuordnen möchten, und drücken SieEingabe.



12. Lesen Sie die Let's-Encrypt-Subscriber-Vereinbarung. Y eingeben undEingabe drücken, um die Vereinbarung zu akzeptieren und fortzufahren.

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

Die Aktionen werden ausgeführt, um HTTPS für Ihre Instance zu aktivieren, einschließlich der Anforderung des Zertifikats und der Konfiguration der angegebenen Umleitungen.

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.
```

Ihr Zertifikat wurde erfolgreich ausgestellt und validiert, und die Umleitungen werden erfolgreich für Ihre Instance konfiguriert, wenn eine Meldung ähnlich dem folgenden Beispiel angezeigt wird.

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:
```

Das `bncert`-Tool führt alle 80 Tage vor Ablauf Ihres Zertifikats eine automatische Erneuerung durch. Wiederholen Sie die obigen Schritte, wenn Sie zusätzliche Domänen und Unterdomänen mit Ihrer Instance verwenden möchten und Sie HTTPS für diese Domänen aktivieren möchten.

Sie sind jetzt fertig, HTTPS auf Ihrer Ghost-Instance zu aktivieren. Wenn Sie das nächste Mal mit der von Ihnen konfigurierten Domäne zu Ihrer Ghost-Website navigieren, sollten Sie sehen, dass sie auf die HTTPS-Verbindung umgeleitet wird.

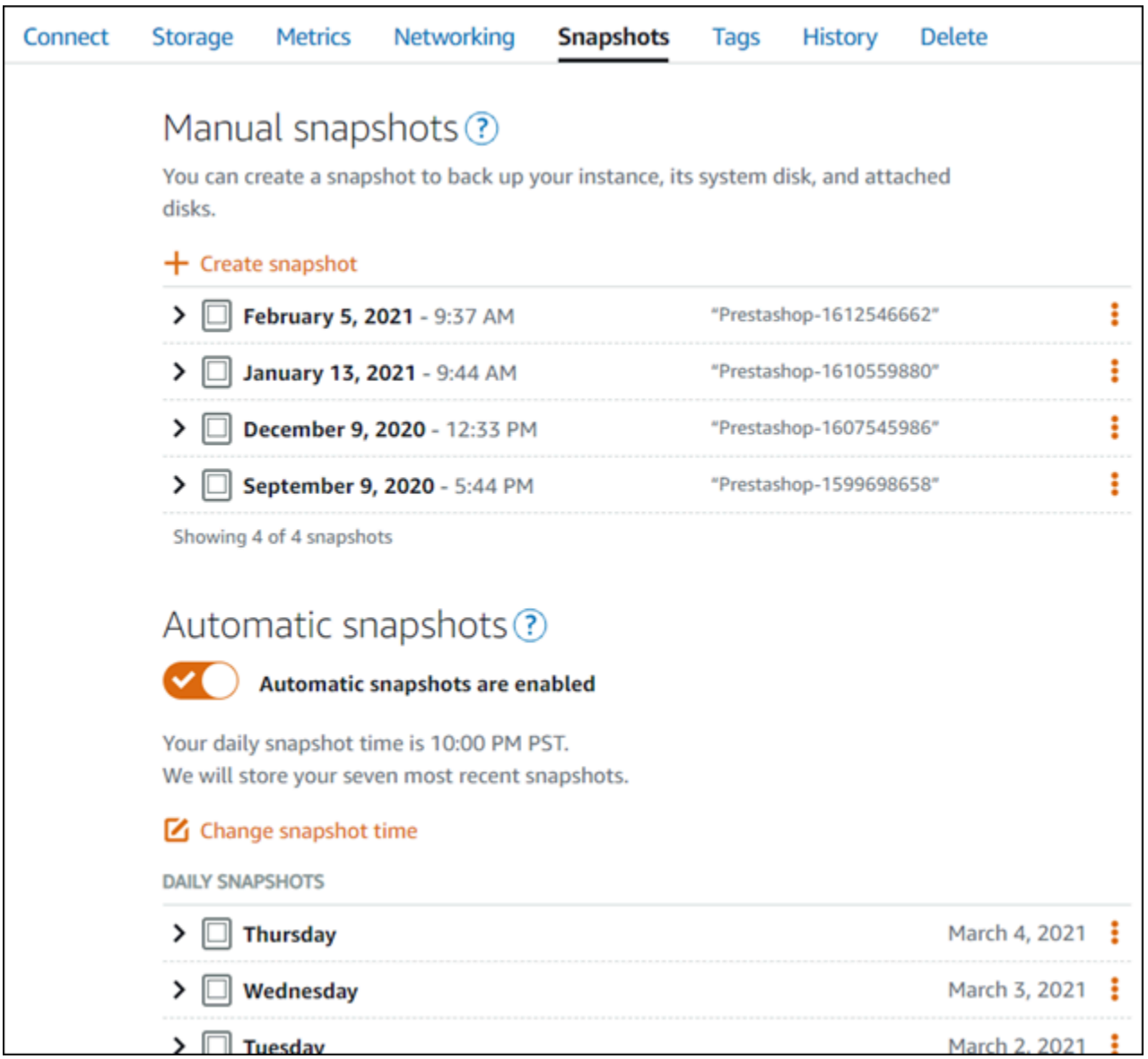
Schritt 7: Die Ghost-Dokumentation lesen und Ihre Website weiter konfigurieren

Lesen Sie die Ghost-Dokumentation, um zu erfahren, wie Sie Ihre Website verwalten und anpassen. Weitere Informationen finden Sie in der Ghost-Dokumentation.

Schritt 8: Einen Snapshot Ihrer Instance erstellen

Nachdem Sie Ihre Ghost-Website so konfiguriert haben, wie Sie sie möchten, erstellen Sie periodische Snapshots Ihrer Instance, um diese zu sichern. Sie können Snapshots manuell erstellen oder automatische Snapshots aktivieren, damit Lightsail tägliche Snapshots für Sie erstellt.. Wenn etwas mit Ihrer Instance nicht stimmt, können Sie mit dem Snapshot eine neue Ersatz-Instance erstellen. Weitere Informationen finden Sie unter Snapshots.

Wählen Sie auf der Instance-Verwaltungsseite, unter der RegisterkarteSnapshotSnapshot erstellenoder wählen Sie aus, automatische Snapshots zu aktivieren.



Weitere Informationen finden Sie unter Erstellen eines Snapshots IhrerLinux- oder Unix-Instance inAmazon LightsailoderAktivieren oder Deaktivieren von automatischen Snapshots für Instances oder Datenträger inAmazon Lightsail.

Schnellstartanleitung: GitLab CE

Hier sind einige erste Schritte, die Sie unternehmen sollten, nachdem Ihre GitLab CE-Instance auf Amazon Lightsail hochgefahren ist und läuft:

Inhalt

- Schritt 2: Abrufen des Standard-Anwendungspassworts für den Zugriff auf den GitLab CE-Administratorbereich
- Schritt 3: Ihrer Instance eine statische IP-Adresse anfügen
- Schritt 4: Beim Admin-Bereich Ihrer Gitlab-CE-Website anmelden
- Schritt 5: Datenverkehr für Ihren registrierten Domänennamen auf Ihre GitLab CE-Website weiterleiten
- Schritt 6: HTTPS für Ihre GitLab CE-Website konfigurieren
- Schritt 7: Die GitLab CE-Dokumentation lesen und Ihre Website weiter konfigurieren
- Schritt 8: Einen Snapshot Ihrer Instance erstellen

Schritt 1: Die Bitnami-Dokumentation lesen

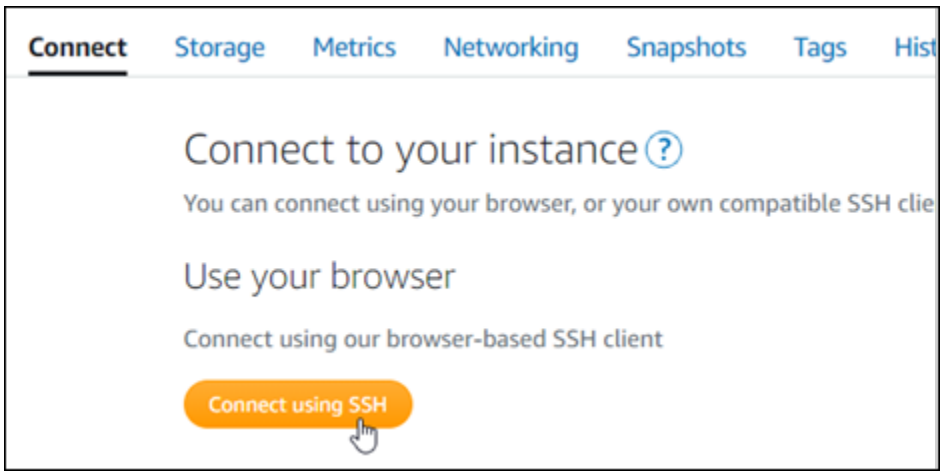
Lesen Sie die Bitnami-Dokumentation, um zu erfahren, wie Sie Ihre GitLab CE-Anwendung konfigurieren. Weitere Informationen finden Sie unter GitLab CE verpackt von Bitnami für AWS Cloud.

Schritt 2: Abrufen des Standard-Anwendungspassworts für den Zugriff auf den GitLab CE-Administratorbereich

Führen Sie das folgende Verfahren aus, um das Standard-Anwendungspasswort für den Zugriff auf den Adminbereich für Ihre GitLab CE-Website zu erhalten. Weitere Informationen finden Sie unter Abrufen des Anwendungsbenutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.

> **Important**
>
> Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um über IPv6 SSH oder RDP in Ihre Instance zu senden. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

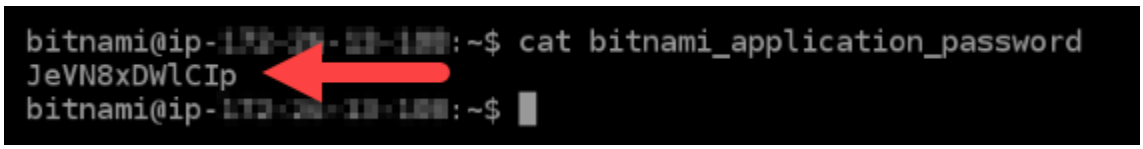
1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um das Anwendungspasswort zu erhalten:

```
cat $HOME/bitnami_application_password
```

Sie sollten eine ähnliche Antwort wie diese sehen, die das Standard-Anwendungspasswort enthält:



Schritt 3: Ihrer Instance eine statische IP-Adresse anfügen

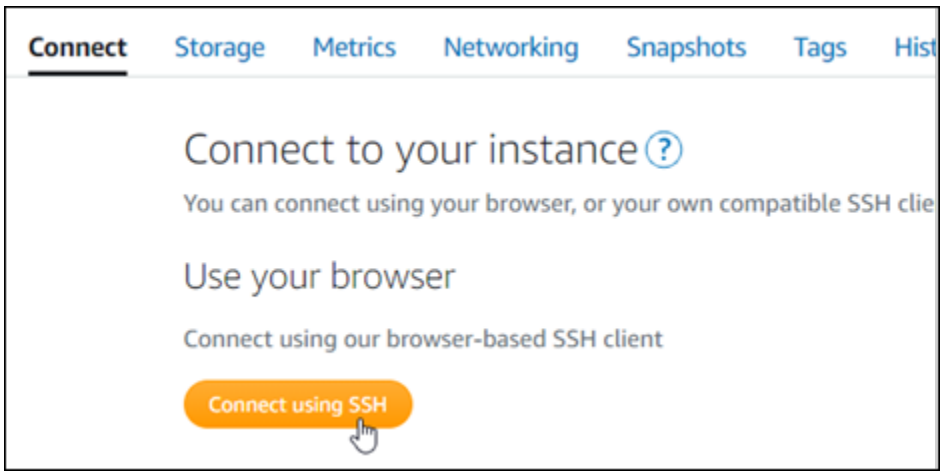
Die Ihrer Instance beim ersten Erstellen zugewiesene öffentliche IP-Adresse ändert sich bei jedem Stopp und Start Ihrer Instance. Sie sollten eine statische IP-Adresse erstellen und an Ihre Instance anfügen, um sicherzustellen, dass sich deren öffentliche IP-Adresse nicht ändert. Wenn Sie Ihrer Instance später einen registrierten Domänennamen wie zum Beispiel `example.com` zuweisen, müssen Sie nicht jedes Mal, wenn Sie Ihre Instance stoppen und neu starten, die DNS-Akte Ihrer Domäne aktualisieren. Sie können eine statische IP an eine Instance anhängen.

Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Netzwerk, die Registerkarte Erstellen einer statischen IP oder Anfügen einer statischen IP (falls Sie zuvor eine statische IP-Adresse erstellt haben, die Sie Ihrer Instance anfügen können) und folgen Sie dann den Anweisungen auf der Seite. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

Nachdem die neue statische IP-Adresse an Ihre Instance angefügt wurde, müssen Sie die folgenden Schritte ausführen, um die Anwendung auf die neue statische IP-Adresse aufmerksam zu machen.

1. Notieren Sie sich die statische IP-Adresse Ihrer Instance. Sie wird im Kopfzeilenabschnitt Ihrer Instance-Verwaltungsseite aufgeführt.

2. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Verbinden die Option Verbinden mit SSH.



3. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein. Stellen Sie sicher, dass Sie *<StaticIP>* mit der neuen statischen IP-Adresse Ihrer Instance ersetzen.

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

Beispiel:

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

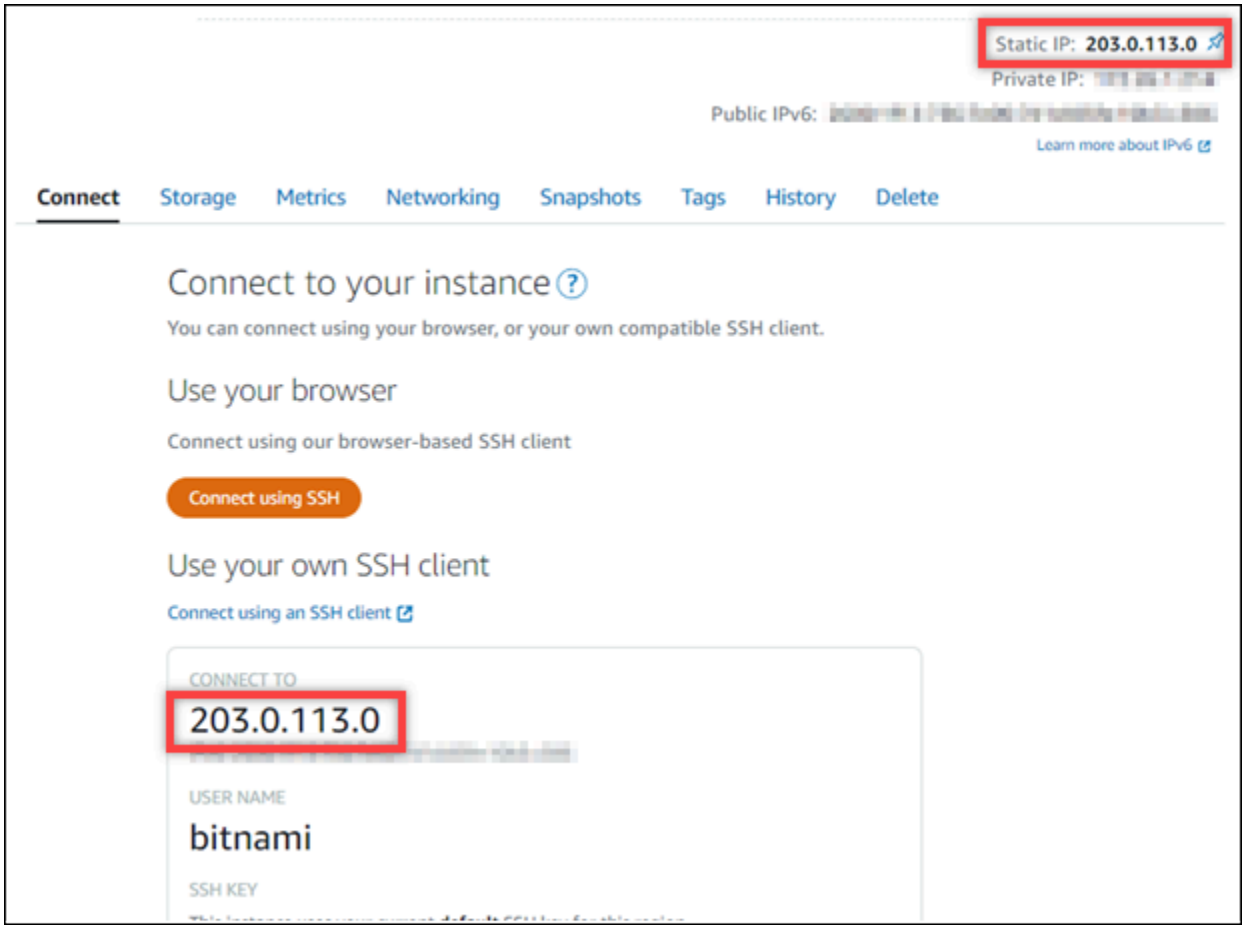
Sie sollten eine Antwort ähnlich dem folgenden Beispiel erhalten. Die Anwendung auf Ihrer Instance sollte nun die neue statische IP-Adresse erkannt haben.

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2022-06-09T16:47:06.737Z - info: Saving configuration info to disk
gitlab 16:47:06.86 INFO  ==> Updating external URL in GitLab configuration
gitlab 16:47:06.88 INFO  ==> Reconfiguring GitLab
gitlab 16:47:45.29 INFO  ==> Starting GitLab services
Disabling automatic domain update for IP address changes
```

Schritt 4: Beim Admin-Bereich Ihrer Gitlab-CE-Website anmelden

Nachdem Sie nun das Standard-Benutzerpasswort haben, navigieren Sie zur Startseite Ihrer GitLab CE-Website und melden Sie sich im Administratorbereich an. Nachdem Sie angemeldet sind, können Sie Ihre Website anpassen und administrative Änderungen vornehmen. Weitere Informationen zu den Möglichkeiten in GitLab CE finden Sie im Abschnitt Schritt 7: Die GitLab CE-Dokumentation lesen und Ihre Website weiter konfigurieren weiter unten in diesem Leitfaden.

1. Notieren Sie sich von Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die öffentliche IP-Adresse Ihrer Instance. Die öffentliche IP-Adresse wird auch im Kopfzeilenabschnitt Ihrer Instance-Verwaltungsseite angezeigt.

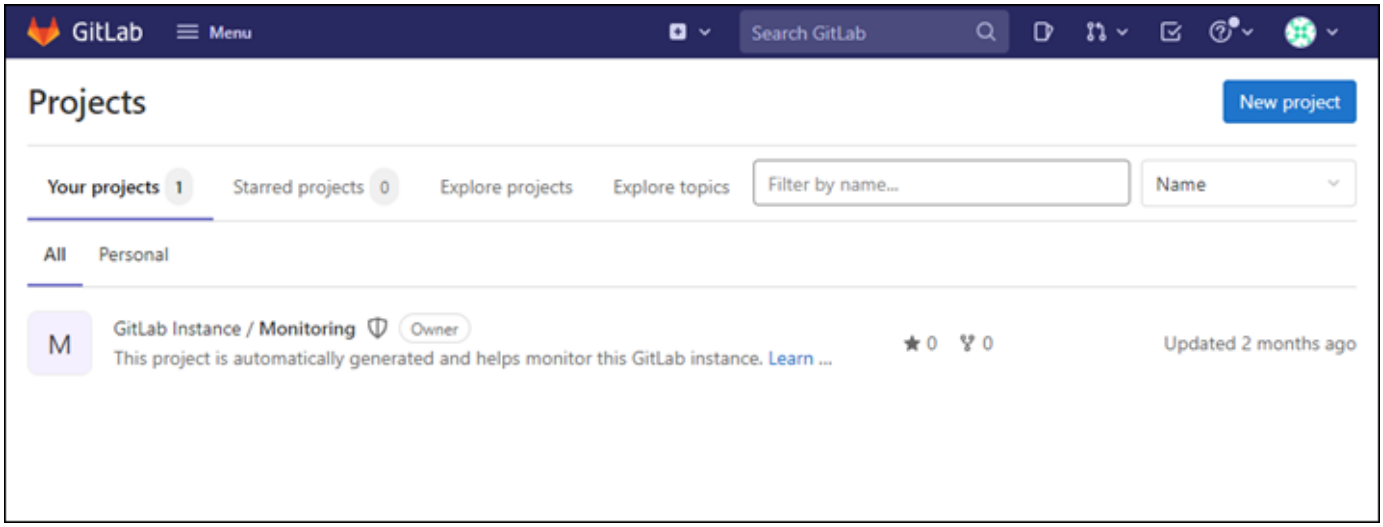


2. Navigieren Sie zur öffentlichen IP-Adresse ihrer Instance, indem Sie z B. zu `http://203.0.113.0` gehen.

   Die Startseite Ihrer Gitlab-CE-Website sollte erscheinen. Möglicherweise warnt Ihr Browser Sie davor, dass Ihre Verbindung nicht privat bzw. sicher ist oder dass ein Sicherheitsrisiko besteht. Dies geschieht, weil auf Ihre GitLab CE-Instance noch kein SSL-/TLS-Zertifikat angewendet wurde. Wählen Sie im Browserfenster Advanced (Erweitert) und dann Details oder More information (Weitere Informationen), um die verfügbaren Optionen anzuzeigen. Besuchen Sie dann die Website, auch wenn diese nicht privat oder sicher ist.

3. Melden Sie sich mit dem Standardbenutzernamen (`root`) und dem zuvor abgerufenen Standardpasswort an, wie vorhin in diesem Leitfaden beschrieben.

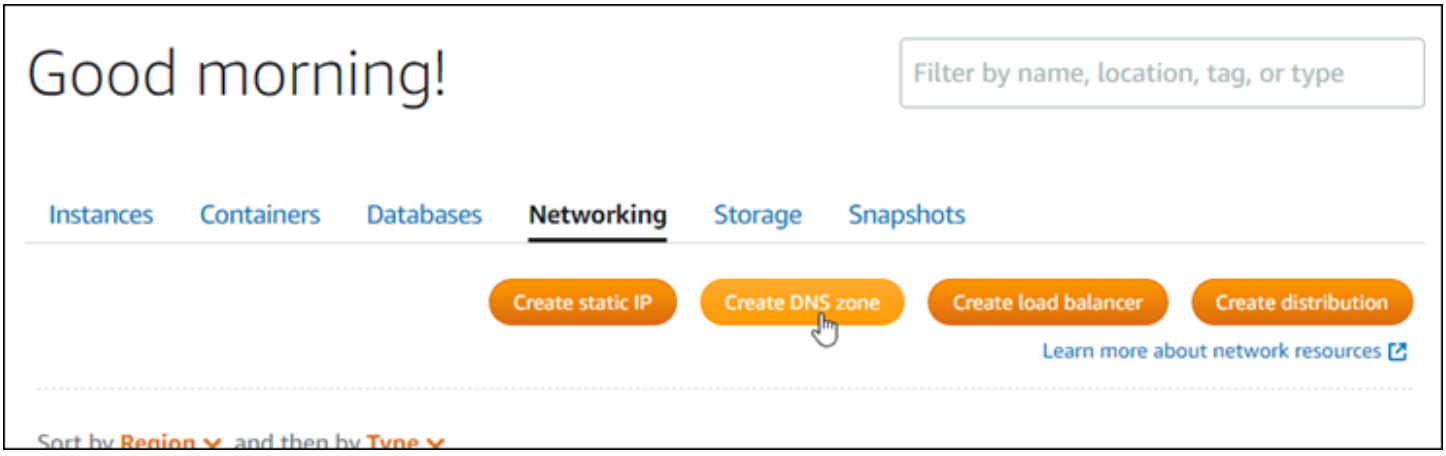
   Das Gitlab-CE-Verwaltungs-Dashboard wird angezeigt.



Schritt 5: Datenverkehr für Ihren registrierten Domänennamen auf Ihre GitLab CE-Website weiterleiten

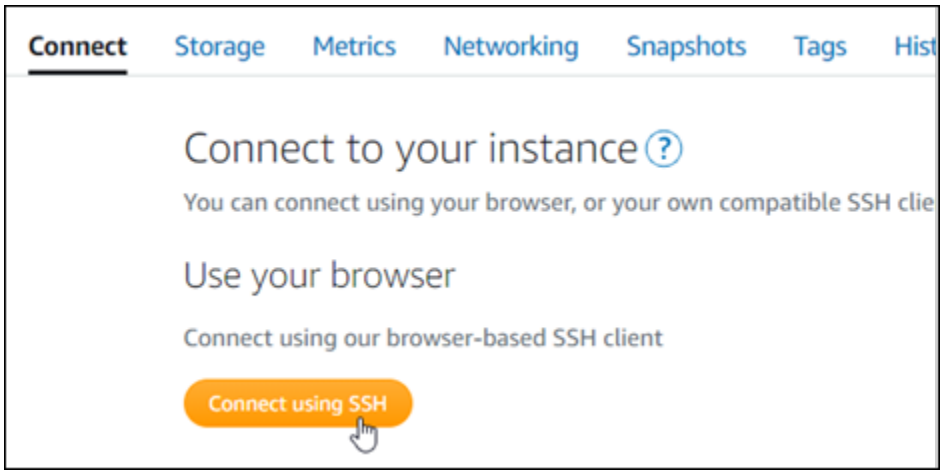
Um den Datenverkehr für Ihren registrierten Domänennamen, z. B. `example.com`, an Ihre GitLab CE-Website weiterzuleiten, fügen Sie dem Domain Name System (DNS) Ihrer Domäne einen Datensatz hinzu. DNS-Datensätze werden in der Regel beim Registrar verwaltet und gehostet, bei dem Sie Ihre Domain registriert haben. Wir empfehlen jedoch, die Verwaltung der DNS-Datensätze Ihrer Domain an Lightsail zu übertragen, damit Sie sie mit der Lightsail-Konsole verwalten können.

Wählen Sie auf der Startseite der Lightsail-Konsole auf der Registerkarte Netzwerk die Option DNS-Zone erstellen aus und folgen Sie dann den Anweisungen auf der Seite. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.



Nachdem Ihr Domänenname Datenverkehr an Ihre Instance weitergeleitet hat, müssen Sie das folgende Verfahren ausführen, um GitLab CE auf den Domänennamen aufmerksam zu machen.

1. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Verbinden die Option Verbinden mit SSH.



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein. Ersetzen Sie *<DomainName>* durch den Domänennamen, der den Datenverkehr an Ihre Instance weiterleitet.

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

Beispiel:

```
sudo /opt/bitnami/configure_app_domain --domain example.com
```

Sie sollten eine Antwort ähnlich dem folgenden Beispiel erhalten. Ihre GitLab CE-Instance sollte nun den Domänennamen kennen.

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain example.com
Configuring domain to example.com
2022-06-09T18:44:00.235Z - info: Saving configuration info to disk
gitlab 18:44:00.36 INFO  ==> Updating external URL in GitLab configuration
gitlab 18:44:00.37 INFO  ==> Reconfiguring GitLab
gitlab 18:44:38.79 INFO  ==> Starting GitLab services
Disabling automatic domain update for IP address changes
```

Wenn dieser Befehl fehlschlägt, verwenden Sie möglicherweise eine ältere Version der GitLab CE-Instance. Versuchen Sie, stattdessen die folgenden Befehle auszuführen. Ersetzen Sie *<DomainName>* durch den Domänennamen, der den Datenverkehr an Ihre Instance weiterleitet.

```
cd /opt/bitnami/apps/gitlab
sudo ./bnconfig --machine_hostname <DomainName>
```

Nachdem diese Befehle ausgeführt wurden, geben Sie den folgenden Befehl ein, um zu verhindern, dass das bnconfig-Tool bei jedem Neustart des Servers automatisch ausgeführt wird.

```
sudo mv bnconfig bnconfig.disabled
```

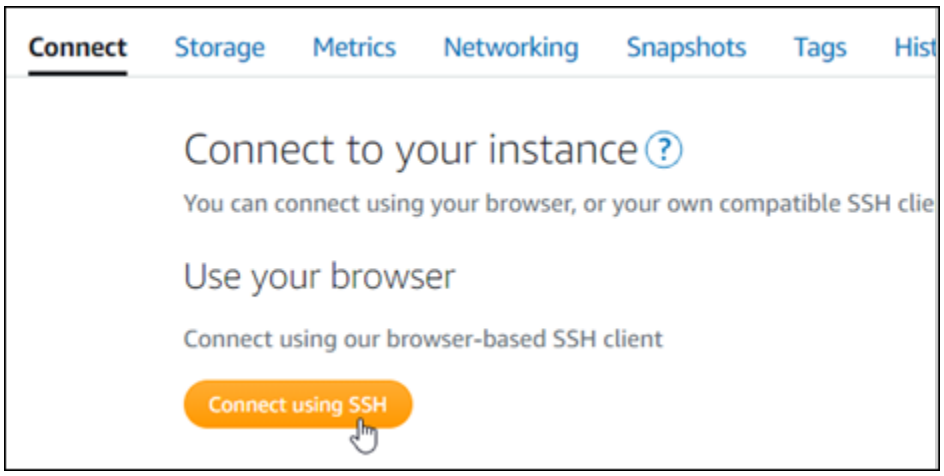
Als Nächstes sollten Sie ein SSL-/TLS-Zertifikat generieren und konfigurieren, um HTTPS-Verbindungen für Ihre GitLab CE-Website zu aktivieren. Weitere Informationen finden Sie im nächsten Abschnitt Schritt 6: HTTPS für Ihre GitLab CE-Website konfigurieren in diesem Leitfaden.

Schritt 6: HTTPS für Ihre GitLab CE-Website konfigurieren

Führen Sie das folgende Verfahren aus, um HTTPS auf Ihrer GitLab CE-Website zu konfigurieren. Diese Schritte zeigen Ihnen, wie Sie den Lego-Client verwenden, ein Befehlszeilentool zum Anfordern von Let's Encrypt SSL/TLS-Zertifikaten.

> **Important**
>
> Bevor Sie mit diesem Verfahren beginnen, stellen Sie sicher, dass Sie Ihre Domain so konfiguriert haben, dass der Datenverkehr an Ihre GitLab CE-Instance weitergeleitet wird. Andernfalls schlägt die SSL/TLS-Zertifikatvalidierung fehl. Um den Datenverkehr für Ihren registrierten Domainnamen auf Ihrer Ghost-Website weiterzuleiten, fügen Sie zum DNS Ihrer Domain einen Datensatz hinzu. DNS-Datensätze werden in der Regel beim Registrar verwaltet und gehostet, bei dem Sie Ihre Domain registriert haben. Wir empfehlen jedoch, die Verwaltung der DNS-Datensätze Ihrer Domain an Lightsail zu übertragen, damit Sie sie mit der Lightsail-Konsole verwalten können.
> Wählen Sie auf der Startseite der Lightsail-Konsole auf der Registerkarte Domains und DNS die Option DNS-Zone erstellen aus und folgen Sie dann den Anweisungen auf der Seite. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain in Lightsail.

1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um das Verzeichnis in das temporäre (/tmp) Verzeichnis zu wechseln.

```
cd /tmp
```

3. Laden Sie die aktuelle Version des Lego-Clients herunter, indem Sie einen der folgenden Befehle eingeben. Dieser Befehl lädt eine Tar-Datei (Bandarchiv) herunter.

```
curl -Ls https://api.github.com/repos/xenolf/lego/releases/latest | grep
 browser_download_url | grep linux_amd64 | cut -d '"' -f 4 | wget -i -
```

4. Verwenden Sie den folgenden Befehl, um die Dateien aus der TAR-Datei zu extrahieren. Ersetzen Sie *X.Y.Z* mit der Version des Lego-Clients, die Sie heruntergeladen haben.

```
tar xf lego_vX.Y.Z_linux_amd64.tar.gz
```

Beispiel:

```
tar xf lego_v4.7.0_linux_amd64.tar.gz
```

5. Verwenden Sie den folgenden Befehl, um das `/opt/bitnami/letsencrypt`-Verzeichnis, in das Sie die Lego-Clientdateien verschieben werden zu erstellen.

```
sudo mkdir -p /opt/bitnami/letsencrypt
```

6. Geben Sie den folgenden Befehl ein, um die Lego-Client-Dateien in das von Ihnen erstellte Verzeichnis zu verschieben.

```
sudo mv lego /opt/bitnami/letsencrypt/lego
```

7. Geben Sie nacheinander die folgenden Befehle ein, um die Anwendungs-Services zu beenden, die auf Ihrer Instance ausgeführt werden.

```
sudo service bitnami stop
sudo service gitlab-runsvdir stop
```

8. Geben Sie den folgenden Befehl ein, um mit dem Lego-Client ein Let's-Encrypt-SSL/TLS-Zertifikat anzufordern.

```
sudo /opt/bitnami/letsencrypt/lego --tls --email="EmailAddress" --
domains="RootDomain" --domains="WwwSubDomain" --path="/opt/bitnami/letsencrypt" run
```

   Ersetzen Sie im Befehl den folgenden Beispielwert mit Ihrem eigenen:

   - *EmailAddress* – Ihre E-Mail-Adresse für Registrierungs-Benachrichtigungen.
   - *RootDomain* – Die primäre Stammdomäne, die den Datenverkehr an Ihre GitLab CE-Website weiterleitet (z. B. `example.com`).
   - *WwwSubDomain* – Die `www` Subdomäne der primären Stammdomäne, die den Datenverkehr an Ihre GitLab CE-Website weiterleitet (z. B. `www.example.com`).

     Sie können mehrere Domänen für Ihr Zertifikat angeben, indem Sie zusätzliche `--domains`-Parameter in Ihrem Befehl angeben. Wenn Sie mehrere Domänen angeben, erstellt Lego ein Zertifikat für alternative Namen (SAN), das dazu führt, dass nur ein Zertifikat für alle von Ihnen angegebenen Domänen gültig ist. Die erste Domäne in Ihrer Liste wird als „CommonName“ des Zertifikats hinzugefügt und der Rest wird als „DNSNames“ zur SAN-Erweiterung innerhalb des Zertifikats hinzugefügt.

   Beispiel:

```
sudo /opt/bitnami/letsencrypt/lego --tls --email="user@example.com" --
domains="example.com" --domains="www.example.com" --path="/opt/bitnami/letsencrypt"
 run
```

9. Drücken Sie Y und Enter (Eingabe) wenn Sie dazu aufgefordert werden die Nutzungsbedingungen zu akzeptieren.

Sie sollten eine Antwort ähnlich dem folgenden Beispiel erhalten.

```
2022/06/09 19:23:27 [INFO] [ example.com ] Server responded with a certificate.
```

Bei Erfolg wird ein Satz von Zertifikaten im `/opt/bitnami/letsencrypt/certificates`-Verzeichnis gespeichert. Dieser Satz enthält die Serverzertifikatdatei (z. B. `example.com.crt`) und die Schlüsseldatei des Serverzertifikats (z. B. `example.com.key`).

10. Geben Sie nacheinander die folgenden Befehle ein, um die vorhandenen Zertifikate auf Ihrer Instance umzubenennen. Später ersetzen Sie diese vorhandenen Zertifikate durch Ihre neuen Let's-Encrypt-Zertifikate.

```
sudo mv /etc/gitlab/ssl/server.crt /etc/gitlab/ssl/server.crt.old
sudo mv /etc/gitlab/ssl/server.key /etc/gitlab/ssl/server.key.old
sudo mv /etc/gitlab/ssl/server.csr /etc/gitlab/ssl/server.csr.old
```

11. Geben Sie nacheinander die folgenden Befehle ein, um symbolische Links für Ihre neuen Let's-Encript-Zertifikate im `/etc/gitlab/ssl` Verzeichnis zu erstellen, das das Standardzertifikatsverzeichnis auf Ihrer GitLab CE-Instance ist.

```
sudo ln -sf /opt/bitnami/letsencrypt/certificates/Domain.key /etc/gitlab/ssl/
server.key
sudo ln -sf /opt/bitnami/letsencrypt/certificates/Domain.crt /etc/gitlab/ssl/
server.crt
```

Ersetzen Sie im Befehl *Domäne* die mit der primären Root-Domäne, die Sie bei der Anforderung Ihrer Let's-Encrypt-Zertifikate angegeben haben.

Beispiel:

```
sudo ln -sf /opt/bitnami/letsencrypt/certificates/example.com.key /etc/gitlab/ssl/
server.key
sudo ln -sf /opt/bitnami/letsencrypt/certificates/example.com.crt /etc/gitlab/ssl/
server.crt
```

12. Geben Sie nacheinander die folgenden Befehle ein, um die Berechtigungen Ihrer neuen Let's-Encrypt-Zertifikate in dem Verzeichnis zu ändern, in das Sie sie verschoben haben.

```
sudo chown root:root /etc/gitlab/ssl/server*
```

```
sudo chmod 600 /etc/gitlab/ssl/server*
```

13. Geben Sie den folgenden Befehl ein, um die Anwendungsservices auf Ihrer GitLab CE-Instance neu zu starten.

```
sudo service bitnami start
```

Wenn Sie das nächste Mal mit der von Ihnen konfigurierten Domain zu Ihrer GitLab CE-Website navigieren, sollten Sie sehen, dass sie zur HTTPS-Verbindung umgeleitet wird. Beachten Sie, dass es bis zu einer Stunde dauern kann, bis die GitLab CE-Instance die neuen Zertifikate erkennt. Wenn Ihre GitLab CE-Website Ihre Verbindung ablehnt, halten Sie die Instance an, starten Sie sie und versuchen Sie es erneut.

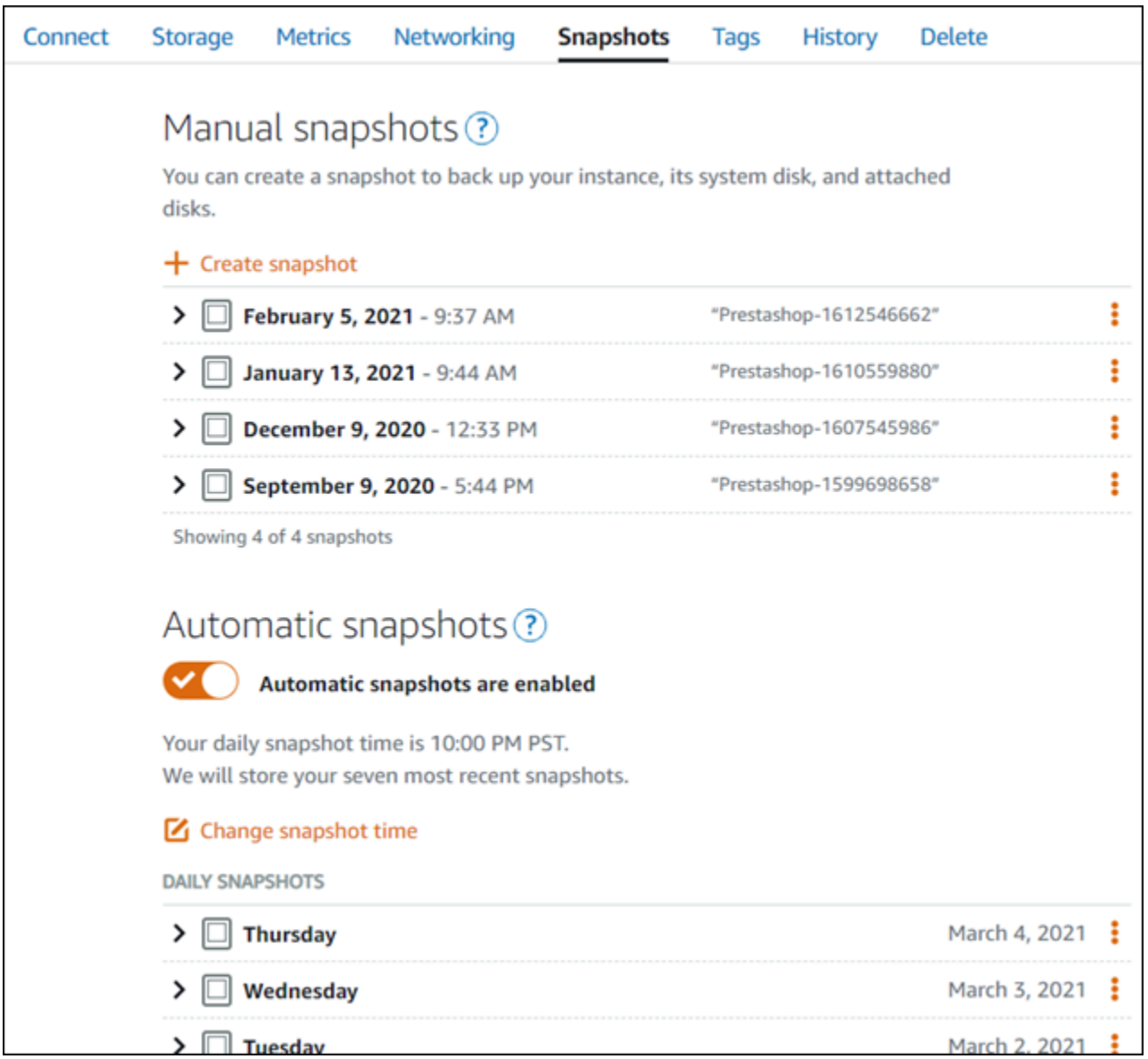
Schritt 7: Die GitLab CE-Dokumentation lesen und Ihre Website weiter konfigurieren

Lesen Sie die GitLab CE-Dokumentation, um zu erfahren, wie Sie Ihre Website verwalten und anpassen. Weitere Informationen finden Sie in der GitLab -Dokumentation.

Schritt 8: Einen Snapshot Ihrer Instance erstellen

Nachdem Sie Ihre GitLab CE-Website so konfiguriert haben, wie Sie sie möchten, erstellen Sie regelmäßig Snapshots Ihrer Instance, um sie zu sichern. Sie können Snapshots manuell erstellen oder automatische Snapshots aktivieren, damit Lightsail tägliche Snapshots für Sie erstellt. Wenn etwas mit Ihrer Instance nicht stimmt, können Sie mit dem Snapshot eine neue Ersatz-Instance erstellen. Weitere Informationen finden Sie unter Snapshots.

Wählen Sie auf der Instance-Verwaltungsseite, unter der RegisterkarteSnapshotSnapshot erstellenoder wählen Sie aus, automatische Snapshots zu aktivieren.



Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Linux- oder Unix-Instance in Amazon Lightsail oder Aktivieren oder Deaktivieren automatischer Snapshots für Instances oder Datenträger in Amazon Lightsail.

Schnellstart-Leitfaden: Joomla!

Hier finden Sie einige erste Schritte, die Sie unternehmen sollten, nachdem Ihre Joomla-Instance auf Amazon Lightsail hochgefahren ist und läuft:

Inhalt

- Schritt 2: Das Standard-Anwendungspasswort für den Zugriff auf die Joomla!-Systemsteuerung einholen
- Schritt 3: Ihrer Instance eine statische IP-Adresse anfügen
- Schritt 4: Bei der Systemsteuerung für Ihre Joomla!-Webseite anmelden
- Schritt 5: Datenverkehr für Ihren registrierten Domänennamen auf Ihre Joomla!-Website weiterleiten
- Schritt 6: HTTPS für Ihre Joomla!-Website konfigurieren
- Schritt 7: Die Joomla!-Dokumentation lesen und konfigurieren Ihre Website weiter konfigurieren
- Schritt 8: Einen Snapshot Ihrer Instance erstellen

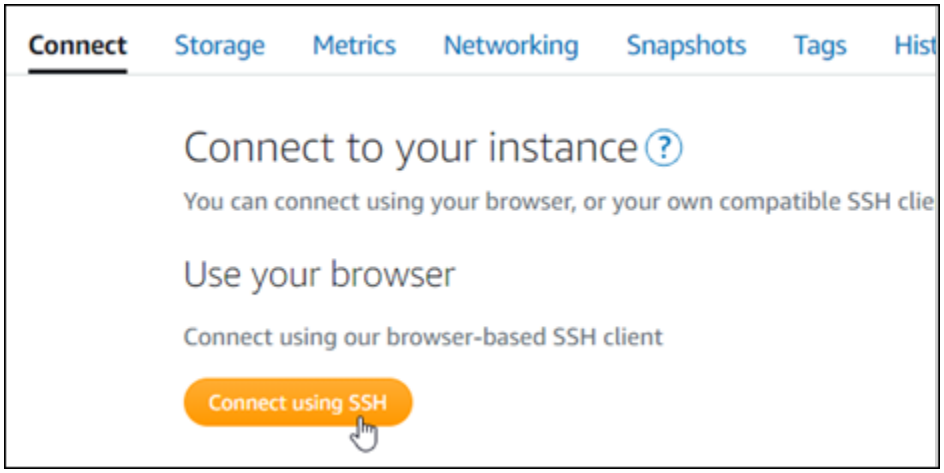
Schritt 1: Die Bitnami-Dokumentation lesen

Lesen Sie die Bitnami-Dokumentation, um zu erfahren, wie Sie Ihre Joomla!-Anwendung konfigurieren. Weitere Informationen finden Sie in der Joomla!- Verpackt von Bitnami für AWS Cloud.

Schritt 2: Das Standard-Anwendungspasswort für den Zugriff auf die Joomla!-Systemsteuerung einholen

Führen Sie das folgende Verfahren durch, um das Standard-Anwendungspasswort für den Zugriff auf die Systemsteuerung für Ihre Joomla!-Webseite zu erhalten. Weitere Informationen finden Sie unter Abrufen des Anwendungs-Benutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.

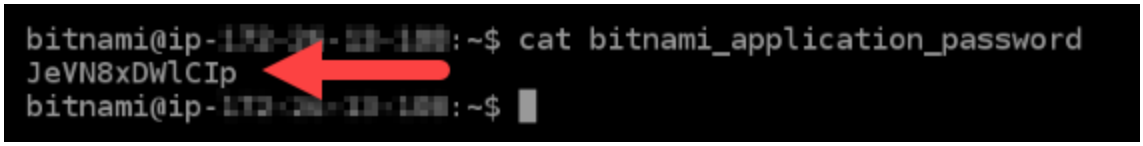
1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um das Anwendungspasswort zu erhalten:

```
cat $HOME/bitnami_application_password
```

Sie sollten eine ähnliche Antwort wie diese sehen, die das Standard-Anwendungspasswort enthält:



Schritt 3: Ihrer Instance eine statische IP-Adresse anfügen

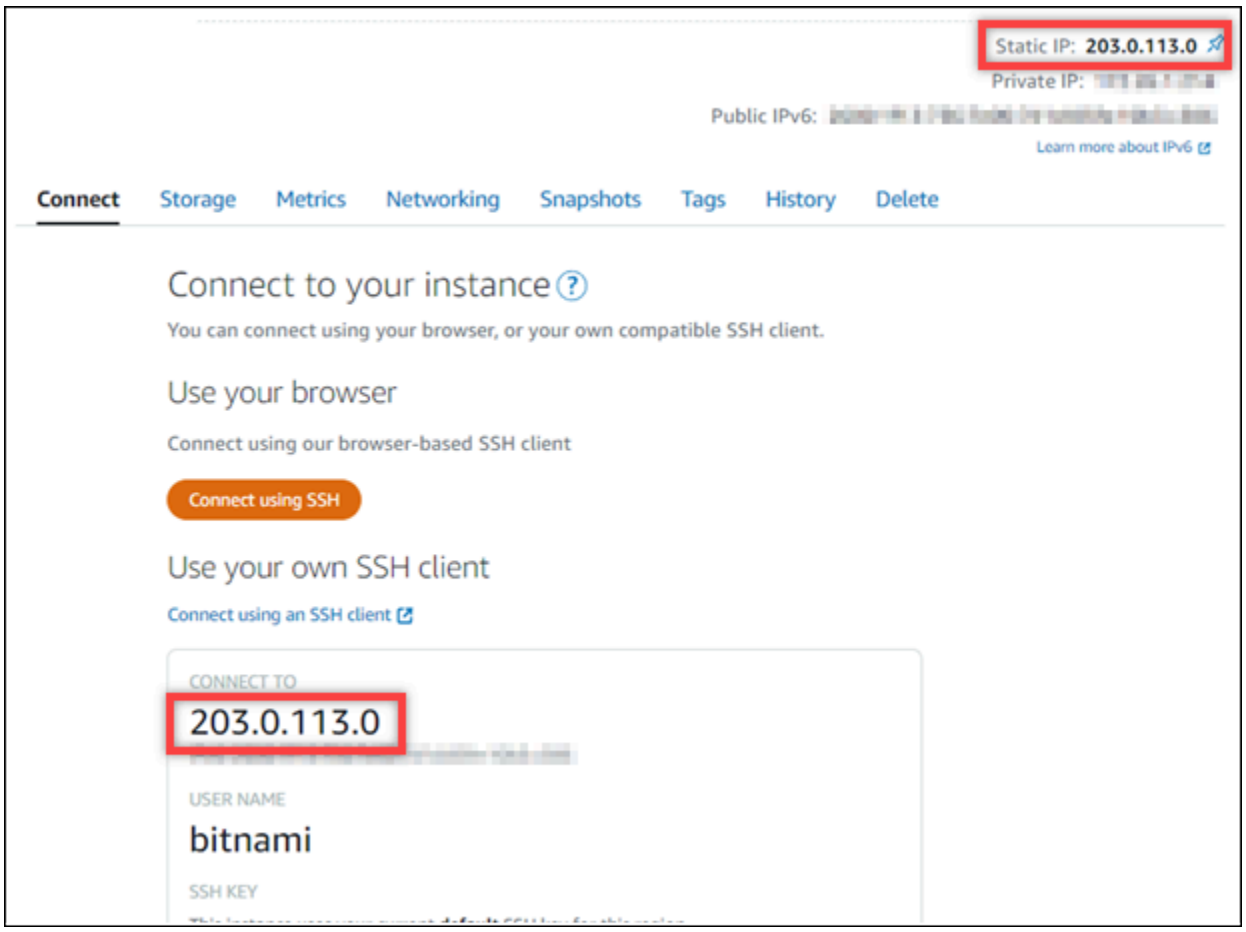
Die Ihrer Instance beim ersten Erstellen zugewiesene öffentliche IP-Adresse ändert sich bei jedem Stopp und Start Ihrer Instance. Sie sollten eine statische IP-Adresse erstellen und an Ihre Instance anfügen, um sicherzustellen, dass sich deren öffentliche IP-Adresse nicht ändert. Wenn Sie Ihrer Instance später einen registrierten Domänennamen wie zum Beispiel `example.com` zuweisen, müssen Sie nicht jedes Mal, wenn Sie Ihre Instance stoppen und neu starten, die DNS-Akte Ihrer Domäne aktualisieren. Sie können eine statische IP an eine Instance anhängen.

Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Netzwerk, die Registerkarte Erstellen einer statischen IP oder Anfügen einer statischen IP (falls Sie zuvor eine statische IP-Adresse erstellt haben, die Sie Ihrer Instance anfügen können) und folgen Sie dann den Anweisungen auf der Seite. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

Schritt 4: Bei der Systemsteuerung für Ihre Joomla!-Webseite anmelden

Nachdem Sie nun das Standard-Anwendungspasswort haben, führen Sie das folgende Verfahren aus, um zur Homepage Ihrer Joomla!-Website zu navigieren und sich bei der Systemsteuerung anzumelden. Nachdem Sie angemeldet sind, können Sie Ihre Website anpassen und administrative Änderungen vornehmen. Weitere Informationen zu den Möglichkeiten in Joomla! finden Sie im Abschnitt Schritt 7: Die Joomla!-Dokumentation lesen und Ihre Website weiter konfigurieren weiter unten in diesem Leitfaden.

1. Notieren Sie sich von Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die öffentliche IP-Adresse Ihrer Instance. Die öffentliche IP-Adresse wird auch im Kopfzeilenabschnitt Ihrer Instance-Verwaltungsseite angezeigt.



2. Navigieren Sie zur öffentlichen IP-Adresse ihrer Instance, indem Sie z B. zu `http://203.0.113.0` gehen.

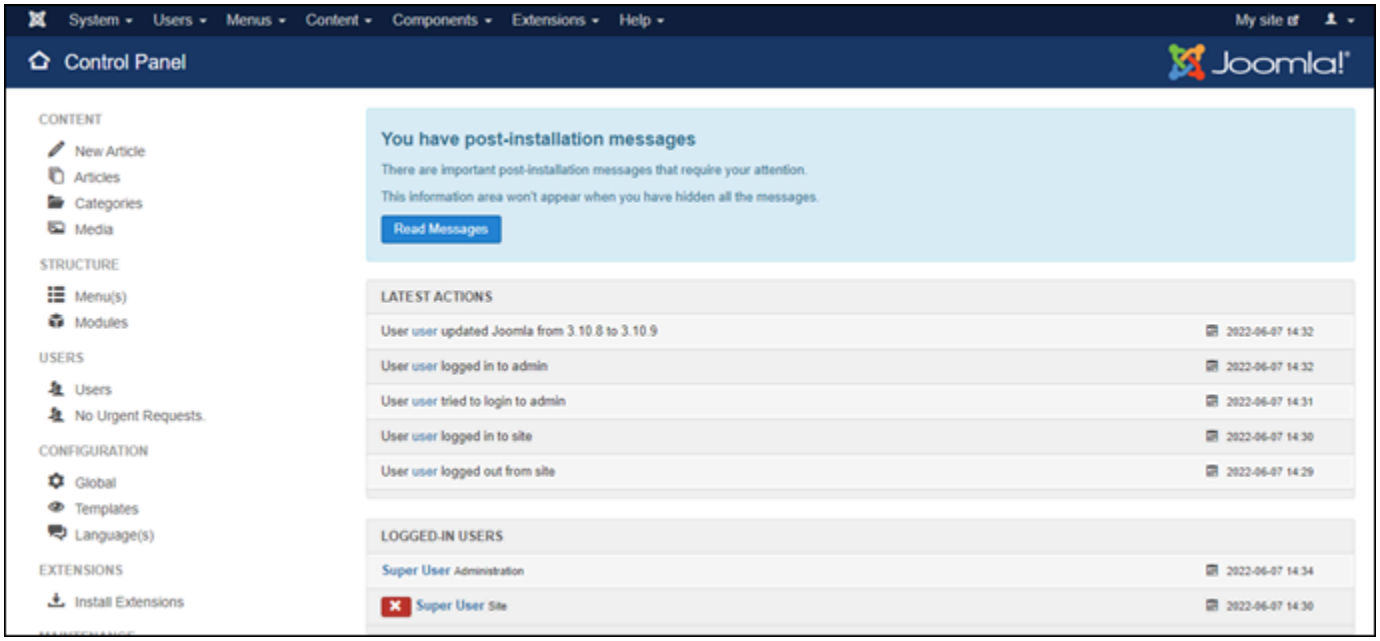
   Die Startseite Ihrer Joomla!-Website sollte erscheinen.

3. Wählen Sie Manage (Verwalten) in der unteren rechten Ecke Ihrer Startseite der Joomla!-Website.

   Wenn das Banner Manage (Verwalten) nicht angezeigt wird, können Sie die Anmeldeseite erreichen, indem Sie zu `http://<PublicIP>/administrator/` gehen. Ersetzen Sie *`<PublicIP>`* durch die öffentliche IP-Adresse Ihrer Instance.

4. Melden Sie sich mit dem Standardbenutzernamen (`user`) und dem zuvor abgerufenen Standardpasswort an, wie vorhin in diesem Leitfaden beschrieben.

   Die Joomla!-Verwaltungs-Systemsteuerung erscheint.



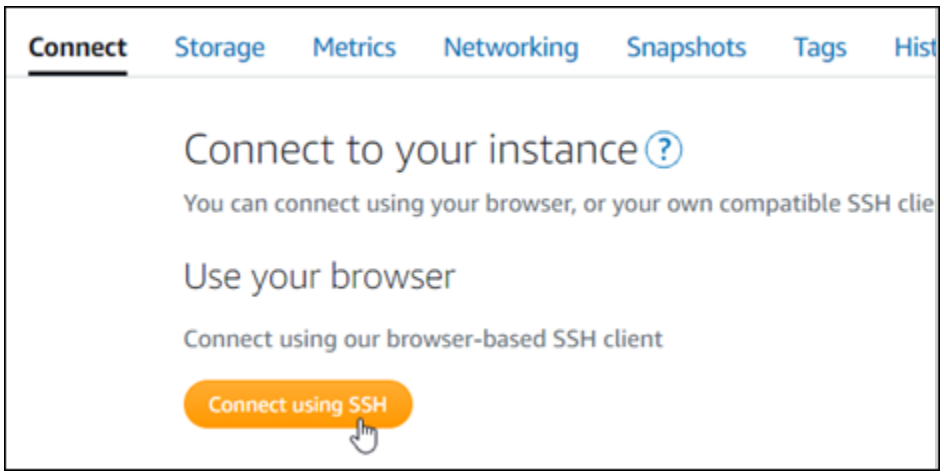
Schritt 5: Datenverkehr für Ihren registrierten Domänennamen auf Ihre Joomla!-Website weiterleiten

Um den Datenverkehr für Ihren registrierten Domainnamen, z. B. `example.com`, auf Ihrer Joomla!-Website weiterzuleiten, fügen Sie zum Domain Name System (DNS) Ihrer Domain einen Datensatz hinzu. DNS-Datensätze werden in der Regel beim Registrar verwaltet und gehostet, bei dem Sie Ihre Domäne registriert haben. Wir empfehlen jedoch, die Verwaltung der DNS-Datensätze Ihrer Domäne auf Lightsail zu übertragen, damit Sie sie über die Lightsail-Konsole verwalten können.

Wählen Sie auf der Startseite der Lightsail-Konsole unter der Registerkarte Domains & DNS (Domains und DNS) die Option Create DNS zone (DNS-Zone erstellen) und folgen Sie dann den Anweisungen auf der Seite. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain in Lightsail.

Nachdem Ihr Domänenname Datenverkehr an Ihre Instance weitergeleitet hat, müssen Sie die folgenden Schritte ausführen, um die Joomla!-Software auf den Domänennamen aufmerksam zu machen.

1. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Verbinden die Option Verbinden mit SSH.



2. Bitnami ist gerade dabei, die Dateistruktur für viele ihrer Vorlagen zu ändern. Die Dateipfade in diesem Tutorial können sich ändern, je nachdem, ob Ihr Bitnami-Vorlage native Linux-Systempakete (Ansatz A) verwendet oder ob es sich um eine eigenständige Installation handelt (Ansatz B). Um Ihren Bitnami-Installationstyp zu identifizieren und zu bestimmen, welchen Ansatz Sie verfolgen sollen, führen Sie den folgenden Befehl aus, nachdem Sie verbunden sind:

```
test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using system
 packages." || echo "Approach B: Self-contained installation."
```

3. Führen Sie die folgenden Schritte aus, wenn das Ergebnis des vorherigen Befehls anzeigte, dass Sie Ansatz A verwenden sollten. Fahren Sie andernfalls mit Schritt 4 fort, wenn das Ergebnis des vorherigen Befehls anzeigte, dass Sie Ansatz B verwenden sollten.

   1. Geben Sie den folgenden Befehl ein, um die virtuelle Host-Konfigurationsdatei für Apache mit Vim zu öffnen und einen virtuellen Host für Ihren Domänennamen zu erstellen.

      ```
      sudo vim /opt/bitnami/apache2/conf/vhosts/joomla-vhost.conf
      ```

   2. Drücken Sie `I`, um den Einfügemodus in Vim einzugeben.
   3. Fügen Sie Ihren Domänenamen hinzu wie im folgenden Beispiel gezeigt wird. In diesem Beispiel verwenden wir die Domänen `example.com` und `www.example.com`.

```
<VirtualHost 127.0.0.1:80 _default_:80>
  ServerName www.example.com
  ServerAlias example.com
  DocumentRoot /opt/bitnami/joomla
  <Directory "/opt/bitnami/joomla">
    Options -Indexes +FollowSymLinks -MultiViews
    AllowOverride None
    Require all granted
  </Directory>
  Include "/opt/bitnami/apache/conf/vhosts/htaccess/joomla-htaccess.conf"
</VirtualHost>
```

4. Drücken Sie die ESC-Taste, und geben Sie dann `:wq!` ein, um Ihre Änderungen zu speichern (schreiben) und Vim zu beenden.
5. Geben Sie den folgenden Befehl ein, um den Apache-Server neu zu starten.

```
sudo /opt/bitnami/ctlscript.sh restart apache
```

4. Führen Sie die folgenden Schritte aus, wenn das Ergebnis des vorherigen Befehls angegeben hat, dass Sie Ansatz B verwenden sollten.

1. Geben Sie den folgenden Befehl ein, um die virtuelle Host-Konfigurationsdatei für Apache mit Vim zu öffnen und einen virtuellen Host für Ihren Domänennamen zu erstellen.

```
sudo vim /opt/bitnami/apps/joomla/conf/httpd-vhosts.conf
```

2. Drücken Sie `I`, um den Einfügemodus in Vim einzugeben.
3. Fügen Sie Ihren Domänenamen hinzu wie im folgenden Beispiel gezeigt wird. In diesem Beispiel verwenden wir die Domänen `example.com` und `www.example.com`.

```
<VirtualHost *:80>
  ServerName example.com
  ServerAlias www.example.com
  ...
```

4. Drücken Sie die ESC-Taste, und geben Sie dann `:wq!` ein, um Ihre Änderungen zu speichern (schreiben) und Vim zu beenden.
5. Geben Sie den folgenden Befehl ein, um zu bestätigen, dass die `bitnami-apps-vhosts.conf`-Datei die `httpd-vhosts.conf`-Datei für Joomla! enthält.

```
sudo vim /opt/bitnami/apache2/conf/bitnami/bitnami-apps-vhosts.conf
```

Suchen Sie in der Datei nach der folgenden Zeile. Fügen Sie dies hinzu, wenn dies fehlt.

```
Include "/opt/bitnami/apps/joomla/conf/httpd-vhosts.conf"
```

6. Geben Sie den folgenden Befehl ein, um den Apache-Server neu zu starten.

```
sudo /opt/bitnami/ctlscript.sh restart apache
```

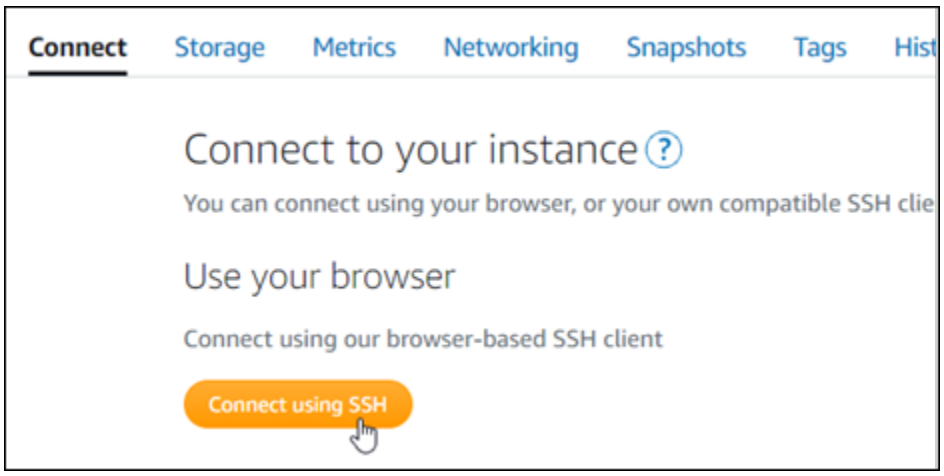
Wenn Sie zu dem Domänennamen navigieren, den Sie für Ihre Instance konfiguriert haben, sollten Sie zur Startseite Ihrer Joomla!-Website umgeleitet werden. Als Nächstes sollten Sie ein SSL/TLS-Zertifikat erstellen und konfigurieren, um HTTPS-Verbindungen für Ihre Joomla!-Website zu ermöglichen. Weitere Informationen erhalten Sie im Abschnitt Schritt 6: HTTPS für Ihre Joomla!-Website konfigurieren in diesem Leitfaden.

Schritt 6: HTTPS für Ihre Joomla!-Website konfigurieren

Führen Sie die folgenden Schritte aus, um HTTPS auf Ihrer Joomla!-Website zu konfigurieren. Diese Schritte zeigen Ihnen, wie Sie das Bitnami-HTTPS-Konfigurations-Tool (`bncert-tool`) verwenden, ein Befehlszeilentool zum Anfordern von SSL/TLS-Zertifikaten von Let's Encrypt. Weitere Informationen finden Sie unter Erfahren Sie mehr über das Bitnami-HTTPS-Konfigurations-Tool in der Bitnami-Dokumentation.

> **Important**
>
> Bevor Sie mit diesem Verfahren beginnen, stellen Sie sicher, dass Sie Ihre Domäne so konfiguriert haben, dass der Datenverkehr an Ihre Joomla!-Instance weitergeleitet wird. Andernfalls schlägt die SSL/TLS-Zertifikatvalidierung fehl.

1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um zu bestätigen, dass das bncert-Tool auf Ihrer Instance installiert ist.

```
sudo /opt/bitnami/bncert-tool
```

Sie sollten eine der folgenden Antworten sehen:

- Wenn Sie den Befehl in der Antwort nicht gefunden haben, ist das bncert-Tool auf Ihrer Instance nicht installiert. Fahren Sie mit dem nächsten Schritt in diesem Verfahren fort, um das bncert-Tool auf Ihrer Instance zu installieren.
- Wenn in der Antwort Willkommen beim HTTPS-Konfigurationstool von Bitnami angezeigt wird, ist das bncert-Tool auf Ihrer Instance installiert. Fahren Sie mit Schritt 8 dieses Verfahrens fort.
- Wenn das bncert-Tool bereits eine Zeit lang auf Ihrer Instance installiert ist, wird möglicherweise eine Meldung angezeigt, die angibt, dass eine aktualisierte Version des Tools verfügbar ist. Wählen Sie, es herunterzuladen, und geben Sie dann den `sudo /opt/bitnami/bncert-tool`-Befehl ein, um das bncert-Tool erneut auszuführen. Fahren Sie mit Schritt 8 dieses Verfahrens fort.

3. Geben Sie den folgenden Befehl ein, um die bncert-Laufdatei auf Ihre Instance herunterzuladen.

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. Geben Sie den folgenden Befehl ein, um ein Verzeichnis für die bncert-Tool-Laufdatei auf Ihrer Instance zu erstellen.

```
sudo mkdir /opt/bitnami/bncert
```

5. Geben Sie den folgenden Befehl ein, um die bncrt-Laufdatei als ein Programm auszuführen.

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. Geben Sie den folgenden Befehl ein, um einen symbolischen Link zu erstellen, der das bncert-Tool ausführt, wenn Sie den Befehl sudo /opt/bitnami/bncert-tool eingeben.

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

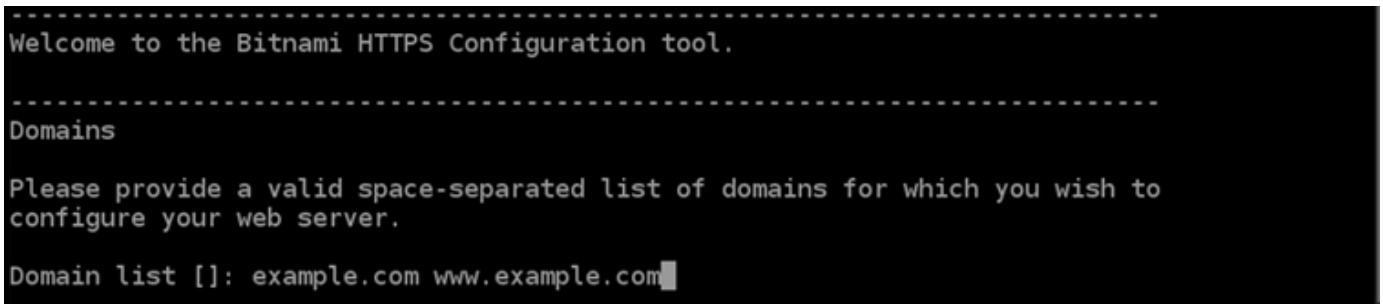
Sie sind jetzt fertig mit der Installation des bncert-Tools auf Ihrer Instance.

7. Geben Sie den folgenden Befehl ein, um das bncert-Tool auszuführen.

```
sudo /opt/bitnami/bncert-tool
```

8. Geben Sie Ihren primären Domänennamen und alternative Domänennamen durch ein Leerzeichen getrennt ein, wie im folgenden Beispiel gezeigt.

Wenn Ihre Domäne nicht darauf konfiguriert ist, Datenverkehr auf die öffentliche IP-Adresse Ihrer Instance umzuleitent, wird das`bncert`-Tool Sie aufgefordern, diese Konfiguration vorzunehmen, bevor Sie fortfahren. Ihre Domäne muss den Datenverkehr an die öffentliche IP-Adresse der Instance weiterleiten, von der Sie das `bncert`-Tool verwenden, um HTTPS für die Instance zu aktivieren. Dies bestätigt, dass Sie Eigentümer der Domäne sind und dient als Validierung für Ihr Zertifikat.

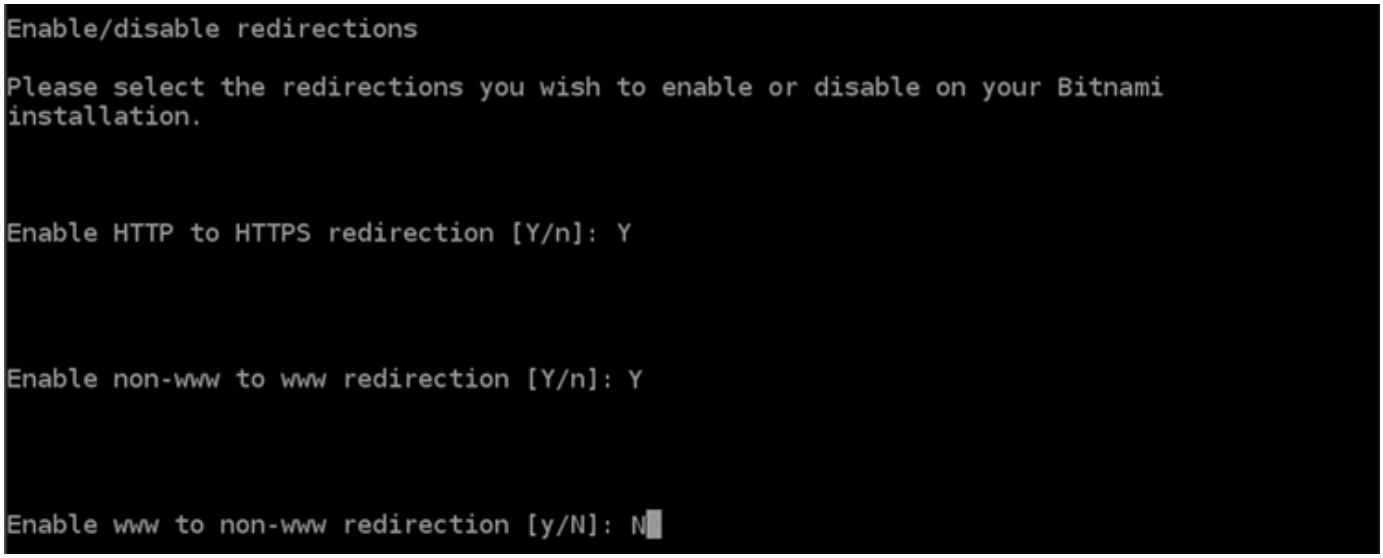


9. Das `bncert`-Tool wird Sie fragen, wie die Umleitung Ihrer Website konfiguriert werden soll. Die folgenden Optionen sind verfügbar:

- Aktivieren einer Umleitung von HTTP zu HTTPS- Gibt an, ob Benutzer, die zur HTTP-Version Ihrer Website navigieren (d. h.`http:/example.com`) automatisch auf die HTTPS-Version umgeleitet (d.h.`https://example.com`) werden. Wir empfehlen, diese Option zu aktivieren, da sie alle Besucher zwingt, die verschlüsselte Verbindung zu verwenden. Y eingeben und Eingabe drücken, um dies zu aktivieren.

- Umleitung von Nicht-www zu www aktivieren- Gibt an, ob Benutzer, die zur Spitze Ihrer Domäne navigieren (d. h.`https://example.com`) automatisch an die`www`Unterdomäne Ihrer Domäne (d. h.`https://www.example.com`) weitergeleitet werden. Wir empfehlen, diese Option zu auszuwählen. Sie können diese jedoch deaktivieren und die alternative Option aktivieren (aktivieren Sie`www` auf Nicht-`www` Umleiten), wenn Sie die Spitze Ihrer Domäne als bevorzugte Website-Adresse in Suchmaschinentools wie den Webmaster-Tools von Google angegeben haben, oder wenn Ihre Spitze direkt auf Ihre IP verweist und Ihre `www` Unterdomäne Ihren Apex über eine CNAME-Akte referenziert. `Y` eingeben und Eingabe drücken, um dies zu aktivieren.
- Umleitung von Nicht-www zu www aktivieren- Gibt an, ob Benutzer, die zur Unterdomäne Ihrer Domäne `www` navigieren (d. h.`https://www.example.com`) automatisch an die Spitze Ihrer Domäne (d. h.`https://example.com`) weitergeleitet werden. Wir empfehlen dies zu deaktivieren, wenn Sie Nicht-`www`Umleiten auf`www` aktiviert haben. `N` eingeben und Eingabe drücken, um dies zu aktivieren.

Ihre Auswahl sollte wie im folgenden Beispiel aussehen.



10. Die Änderungen, die vorgenommen werden, sind aufgelistet. `Y` eingeben und`Eingabe` drücken, um zu bestätigen und fortzufahren.

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
www.example.com)
7. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

11. Geben Sie Ihre E-Mail-Adresse ein, die Sie Ihrem Let's-Encrypt-Zertifikat zuordnen möchten, und drücken SieEingabe.

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

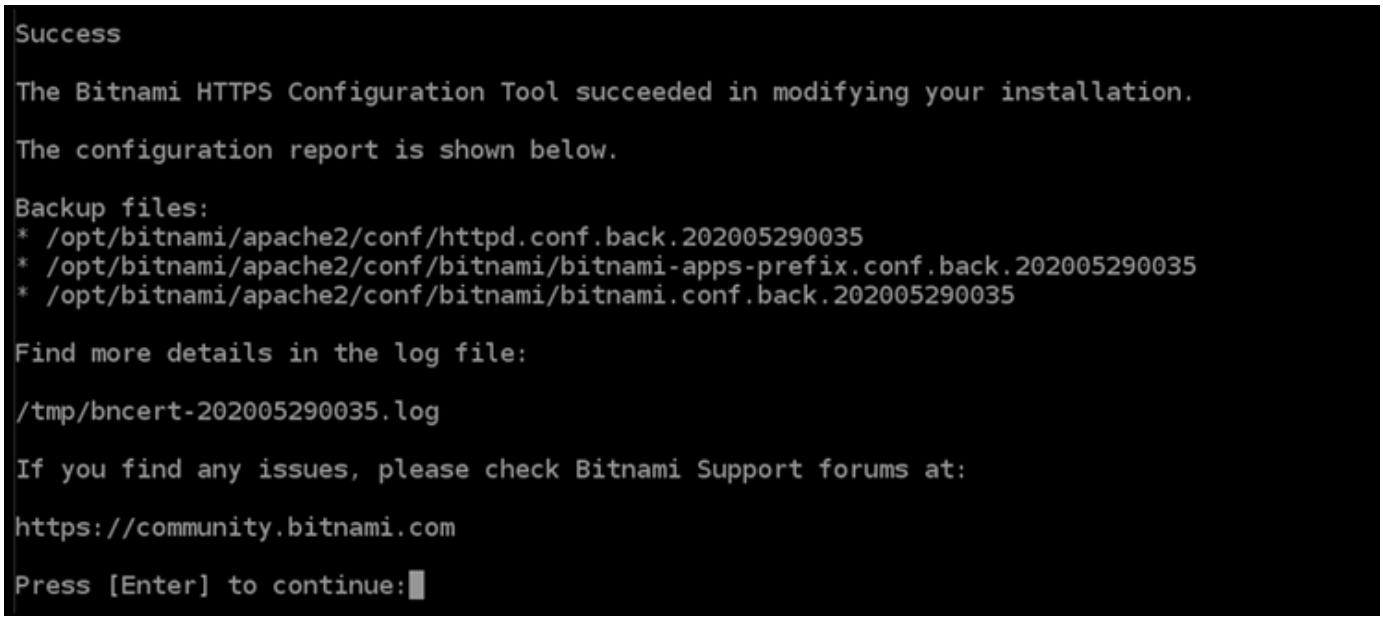
12. Lesen Sie die Let's-Encrypt-Subscriber-Vereinbarung. Y eingeben undEingabe drücken, um die Vereinbarung zu akzeptieren und fortzufahren.

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

Die Aktionen werden ausgeführt, um HTTPS für Ihre Instance zu aktivieren, einschließlich der Anforderung des Zertifikats und der Konfiguration der angegebenen Umleitungen.

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.

|
```

Ihr Zertifikat wurde erfolgreich ausgestellt und validiert, und die Umleitungen werden erfolgreich für Ihre Instance konfiguriert, wenn eine Meldung ähnlich dem folgenden Beispiel angezeigt wird.



Das `bncert`-Tool führt alle 80 Tage vor Ablauf Ihres Zertifikats eine automatische Erneuerung durch. Wiederholen Sie die obigen Schritte, wenn Sie zusätzliche Domänen und Unterdomänen mit Ihrer Instance verwenden möchten und Sie HTTPS für diese Domänen aktivieren möchten.

Sie sind jetzt fertig, HTTPS auf Ihrer Joomla!-Instance zu aktivieren. Wenn Sie das nächste Mal mit der von Ihnen konfigurierten Domäne zu Ihrer Joomla!-Website navigieren, sollten Sie sehen, dass sie auf die HTTPS-Verbindung umgeleitet wird.

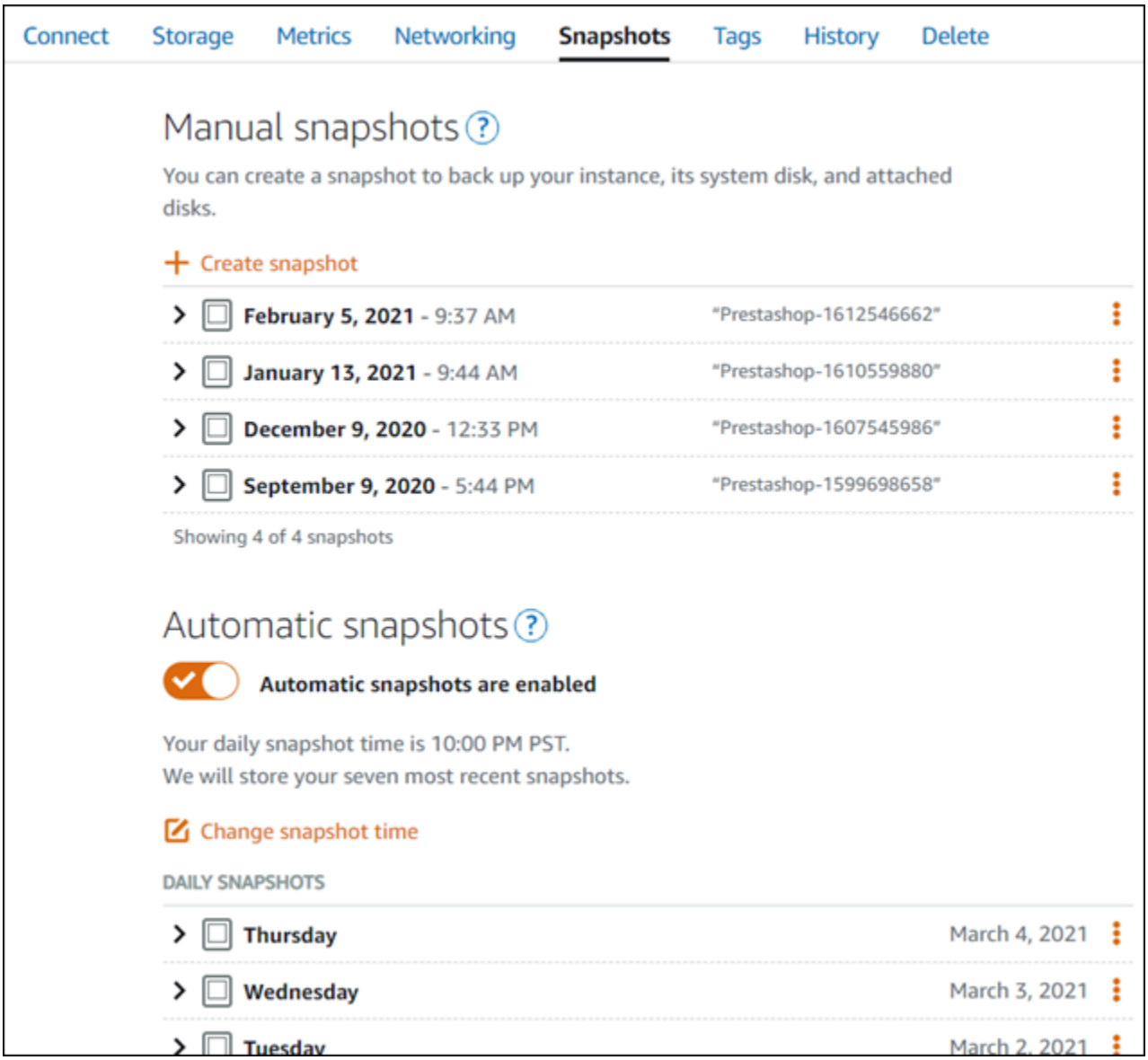
Schritt 7: Die Joomla!-Dokumentation lesen und Ihre Website weiter konfigurieren

Lesen Sie die Joomla!-Dokumentation, um zu erfahren, wie Sie Ihre Website verwalten und anpassen. Weitere Informationen finden Sie in der Joomla!- Dokumentation.

Schritt 8: Einen Snapshot Ihrer Instance erstellen

Nachdem Sie Ihre Joomla!-Website so konfiguriert haben, wie Sie sie möchten, erstellen Sie periodische Snapshots Ihrer Instance, um diese zu sichern. Sie können Snapshots manuell erstellen oder automatische Snapshots aktivieren, damit Lightsail tägliche Snapshots für Sie erstellt.. Wenn etwas mit Ihrer Instance nicht stimmt, können Sie mit dem Snapshot eine neue Ersatz-Instance erstellen. Weitere Informationen finden Sie unter Snapshots.

Wählen Sie auf der Instance-Verwaltungsseite, unter der RegisterkarteSnapshotSnapshot erstellenoder wählen Sie aus, automatische Snapshots zu aktivieren.



Weitere Informationen finden Sie unter Erstellen eines Snapshots IhrerLinux- oder Unix-Instance inAmazon LightsailoderAktivieren oder Deaktivieren von automatischen Snapshots für Instances oder Datenträger inAmazon Lightsail.

Schnellstartanleitung: LAMP

Hier finden Sie einige erste Schritte, die Sie unternehmen sollten, nachdem Ihre LAMP-Instance auf Amazon Lightsail hochgefahren ist und läuft:

Schritt 1: Holen Sie sich das Standard-Anwendungspasswort für Ihre LAMP-Instance

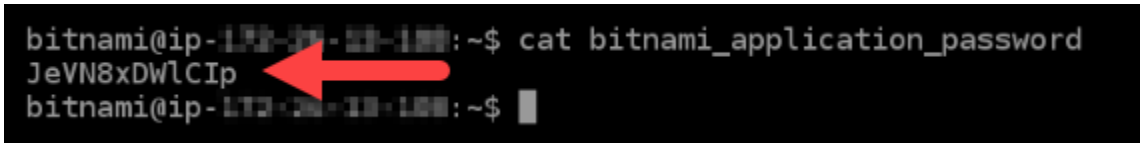
Sie benötigen das Standard-Anwendungspasswort, um auf vorinstallierte Anwendungen oder Dienste auf Ihrer Instance zugreifen zu können.

1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).
2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um das Anwendungspasswort zu erhalten:

   ```
   cat bitnami_application_password
   ```

   > **Note**
   >
   > Wenn Sie sich in einem anderen Verzeichnis als dem Stammverzeichnis des Benutzers befinden, geben Sie `cat $HOME/bitnami_application_password` ein.

   Sie sollten eine ähnliche Antwort wie diese sehen, die das Standard-Anwendungspasswort enthält:

Weitere Informationen finden Sie unter Abrufen des Anwendungs-Benutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.

Schritt 2: Fügen Sie an Ihre LAMP-Instance eine statische IP-Adresse an

Die standardmäßig an Ihre Instance angefügte dynamische öffentliche IP-Adresse ändert sich bei jedem Stopp und Start der Instance. Erstellen Sie eine statische IP-Adresse und fügen Sie sie an Ihre Instance an, damit die öffentliche IP-Adresse nicht mehr geändert wird. Später, wenn Sie Ihren Domänennamen mit Ihrer Instance verwenden, müssen Sie die DNS-Datensätze Ihrer Domäne nicht jedes Mal aktualisieren, wenn Sie die Instance stoppen und starten. Sie können eine statische IP an eine Instance anhängen.

Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Networking (Netzwerk) die Option Create static IP (Statische IP erstellen) und folgen Sie dann den Anweisungen auf der Seite.

Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

Schritt 3: Besuchen Sie die Startseite Ihrer LAMP-Instance

Navigieren Sie zur öffentlichen IP-Adresse Ihrer Instance, um auf die darauf installierte Anwendung zuzugreifen, auf phpMyAdmin oder auf die Bitnami-Dokumentation.

1. Notieren Sie sich von Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die öffentliche IP-Adresse.
2. Navigieren Sie zur öffentlichen IP-Adresse, indem Sie z. B. zu `http://192.0.2.3` gehen.

Weitere Informationen finden Sie unter Abrufen des Anwendungs-Benutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.

Schritt 4: Ordnen Sie Ihren Domänennamen Ihrer LAMP-Instance zu

Um Ihren Domänennamen, wie z. B. `example.com`, auf Ihre Instance abzubilden, fügen Sie einen Datensatz zum Domain Name System (DNS) Ihrer Domäne hinzu. DNS-Datensätze werden in der Regel beim Registrar verwaltet und gehostet, bei dem Sie Ihre Domäne registriert haben. Wir empfehlen jedoch, die Verwaltung der DNS-Datensätze Ihrer Domäne auf Lightsail zu übertragen, damit Sie sie über die Lightsail-Konsole verwalten können.

Wählen Sie auf der Startseite der Lightsail-Konsole unter der Registerkarte Domains & DNS (Domains und DNS) die Option Create DNS zone (DNS-Zone erstellen) und folgen Sie dann den Anweisungen auf der Seite.

Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain in Lightsail.

Schritt 5: Lesen Sie die Bitnami-Dokumentation

Lesen Sie die Bitnami-Dokumentation, um zu erfahren, wie Sie Ihre Anwendung bereitstellen, die HTTP-Unterstützung mit SSL-Zertifikaten aktivieren, Dateien mit SFTP auf den Server hochladen und vieles mehr.

Weitere Informationen finden Sie unter Bitnami LAMP für die AWS Cloud.

Schritt 6: Erstellen Sie einen Snapshot Ihrer LAMP-Instance

Ein Snapshot ist eine Kopie des Systemlaufwerks und der ursprünglichen Konfiguration einer Instance. Der Snapshot enthält Informationen wie Speicher, CPU, Festplattengröße und Datenübertragungsrate. Sie können einen Snapshot als Grundlage für neue Instances oder als Datensicherung verwenden.

Geben Sie auf Ihrer Instance-Verwaltungsseite auf der Registerkarte Snapshot einen Namen für den Snapshot ein und wählen Sie dann Create snapshot (Snapshot erstellen) aus.

Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Linux- oder Unix-Instance.

Schnellstartanleitung: Magento

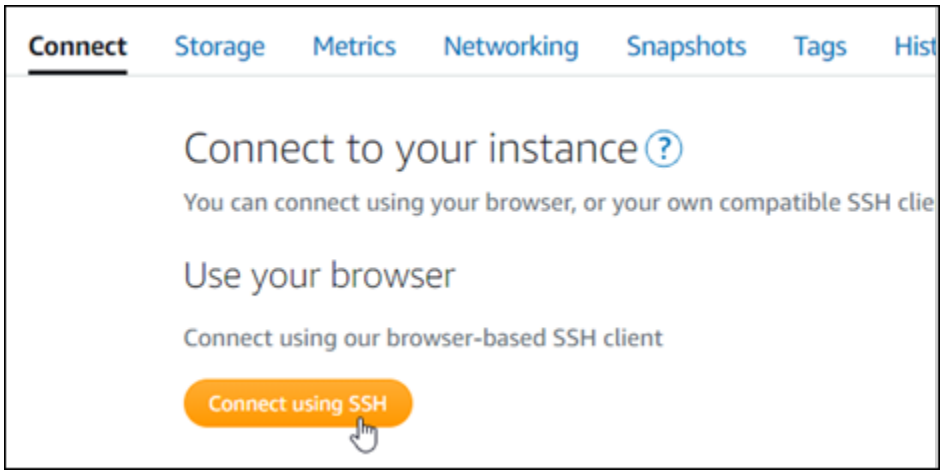
Hier finden Sie einige erste Schritte, die Sie ausführen sollten, nachdem Ihre Magento-Instance auf Amazon Lightsail hochgefahren ist und läuft.

Inhalt

Schritt 1: Das Standard-Anwendungspasswort für Ihre Magento-Website einholen

Führen Sie die folgenden Schritte aus, um das Standard-Anwendungspasswort für Ihre Magento-Website zu erhalten. Weitere Informationen finden Sie unter Abrufen des Anwendungs-Benutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.

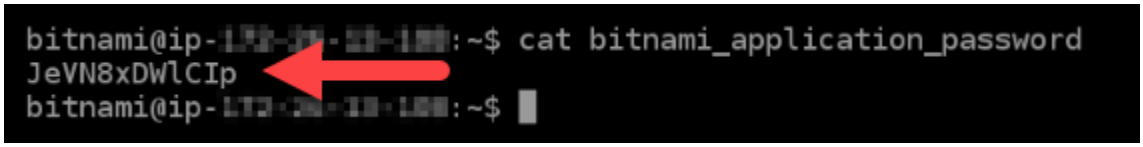
1. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Verbinden die Option Verbinden mit SSH.



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um das Standard-Anwendungspasswort zu erhalten:

```
cat $HOME/bitnami_application_password
```

Sie sollten eine ähnliche Antwort wie diese sehen, die das Standard-Anwendungspasswort enthält. Speichern Sie dieses Passwort an einem sicheren Ort. Sie werden es im nächsten Abschnitt dieses Tutorials verwenden, um sich beim Verwaltungs-Dashboard Ihrer Magento-Website anzumelden.



Schritt 2: Ihrer Magento-Instance eine statische IP-Adresse anfügen

Die Ihrer Instance beim ersten Erstellen zugewiesene öffentliche IP-Adresse ändert sich bei jedem Stopp und Start Ihrer Instance. Sie sollten eine statische IP-Adresse erstellen und an Ihre Instance anfügen, um sicherzustellen, dass sich deren öffentliche IP-Adresse nicht ändert. Wenn Sie Ihrer Instance später einen registrierten Domänennamen wie zum Beispiel `example.com` zuweisen, müssen Sie nicht jedes Mal, wenn Sie Ihre Instance stoppen und neu starten, die DNS-Akte Ihrer Domäne aktualisieren. Sie können eine statische IP an eine Instance anhängen.

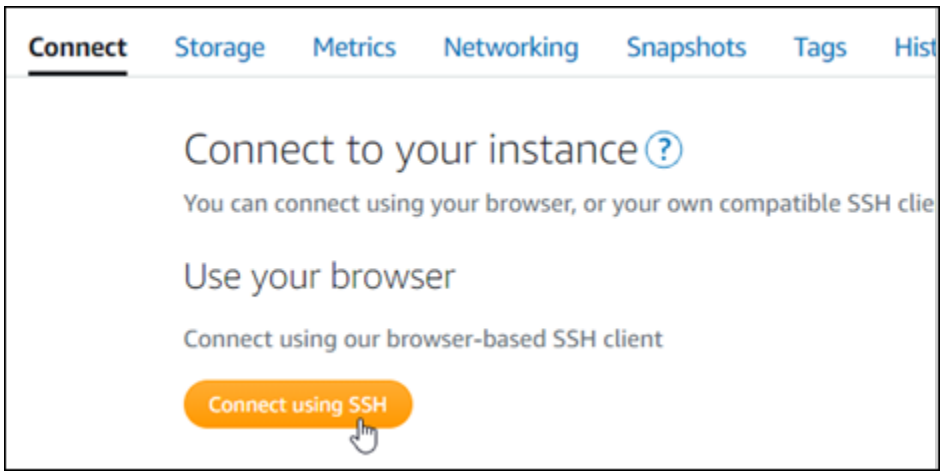
Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Netzwerk, die Registerkarte Erstellen einer statischen IP oder Anfügen einer statischen IP (falls Sie zuvor eine statische

IP-Adresse erstellt haben, die Sie Ihrer Instance anfügen können) und folgen Sie dann den Anweisungen auf der Seite. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

Nachdem die neue statische IP-Adresse an Ihre Instance angefügt wurde, müssen Sie die folgenden Schritte ausführen, um die Magento-Software auf die neue statische IP-Adresse aufmerksam zu machen.

1. Notieren Sie sich die statische IP-Adresse Ihrer Instance. Sie wird im Kopfzeilenabschnitt Ihrer Instance-Verwaltungsseite aufgeführt.

2. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Verbinden die Option Verbinden mit SSH.



3. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein. Stellen Sie sicher, dass Sie*<StaticIP>* mit der neuen statischen IP-Adresse Ihrer Instance ersetzen.

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

Beispiel:

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

Sie sollten eine Reaktion ähnlich dem folgenden Beispiel erhalten. Die Magento-Software sollte nun die neue statische IP-Adresse erkannt haben.

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

> **Note**
>
> Derzeit unterstützt Magento keine IPv6-Adressen. Sie können IPv6 für die Instance aktivieren, aber die Magento-Software reagiert nicht auf Anfragen über das IPv6-Netzwerk.

Schritt 3: Beim Verwaltungs-Dashboard für Ihre Magento-Website anmelden

Führen Sie die folgenden Schritte aus, um auf Ihre Magento-Website Zugriff zu haben und sich beim Verwaltungs-Dashboard anzumelden. Um sich anzumelden, verwenden Sie den Standard-Benutzernamen (`user`) und das Standard-Anwendungspasswort, das Sie zuvor in diesem Leitfaden erhalten haben.

1. Notieren Sie sich in derLightsail-Konsole, die öffentliche oder statische IP-Adresse, die im Kopfzeilenabschnitt der Instance-Verwaltungsseite aufgeführt ist.

2. Navigieren Sie zu der folgenden Adresse, um die Anmeldeseite für das Verwaltungs-Dashboard Ihrer Magento-Website aufzurufen. Stellen Sie sicher, dass Sie *<InstanceIpAddress>* mit der öffentlichen oder statischen IP-Adresse Ihrer Instance ersetzen.

```
http://<InstanceIpAddress>/admin
```

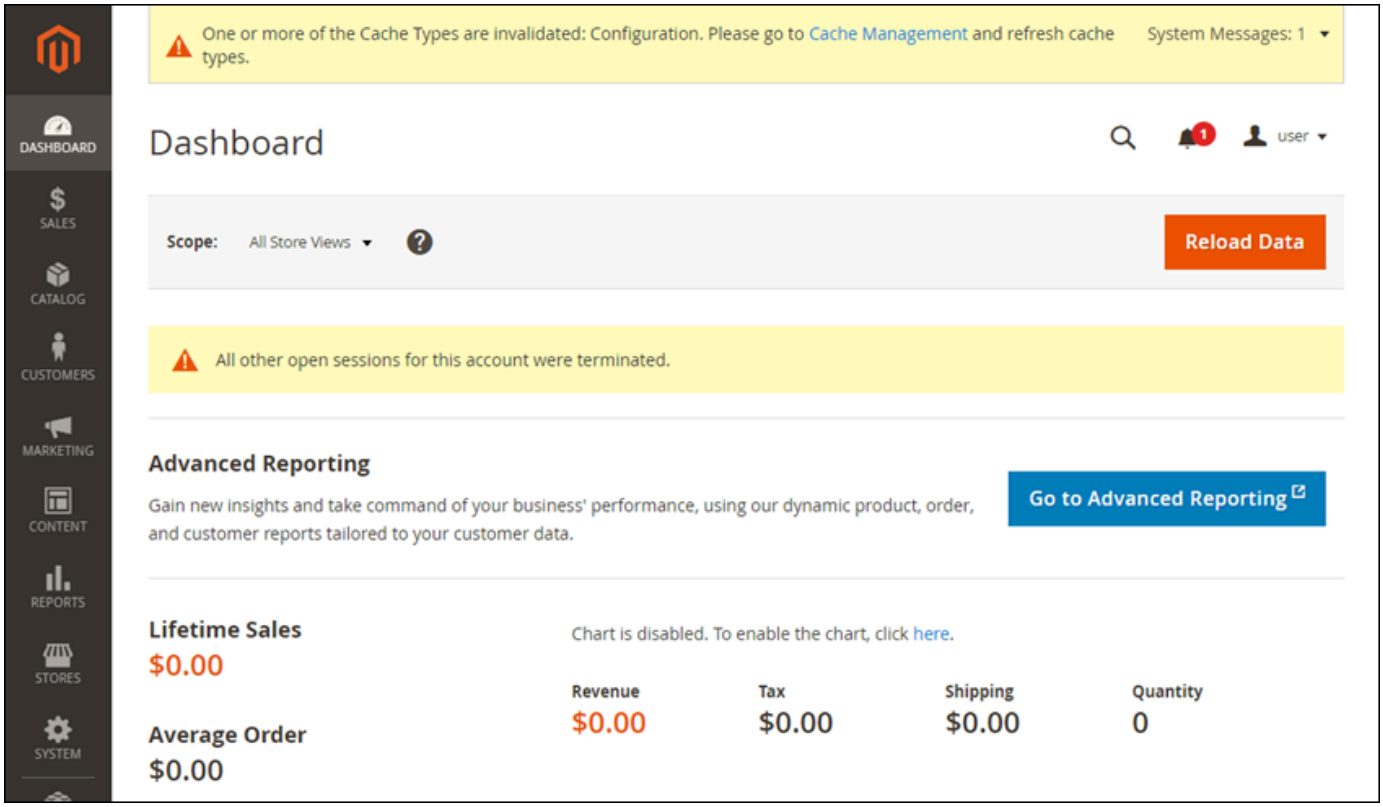
   Beispiel:

```
http://203.0.113.0/admin
```

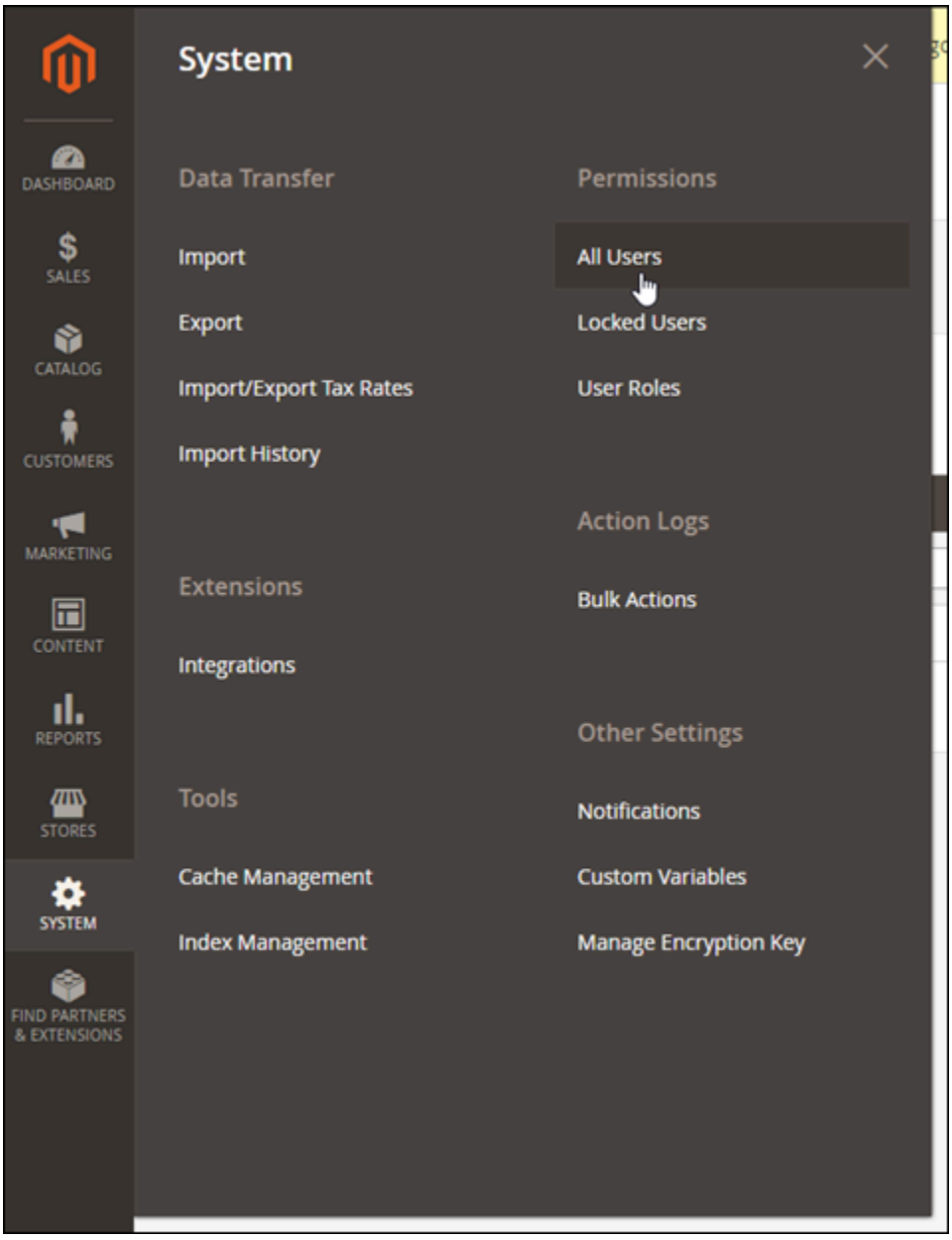
   > **Note**
   >
   > Möglicherweise müssen Sie die Instance neu starten, wenn Sie nicht auf die Anmeldeseite für das Magento-Administrations-Dashboard zugreifen können.

3. Geben Sie den Standard-Benutzernamen ein (`user`), das Standard-Anwendungspasswort, das Sie zuvor in diesem Leitfaden erhalten haben, und wählen Sie Sign in (Anmelden) aus.

Das Magento-Verwaltungs-Dashboard wird angezeigt.



Um den Standard-Benutzernamen oder -Passwort zu ändern, mit dem Sie sich beim Verwaltungs-Dashboard Ihrer Magento-Website anmelden, wählen Sie System im Navigationsbereich und dann All Users (Alle Benutzer) aus. Weitere Informationen finden Sie unter Benutzer hinzufügen in der Magento-Dokumentation.



Weitere Informationen zum Verwaltungs-Dashboard finden Sie im Magento 2.4-Benutzerhandbuch.

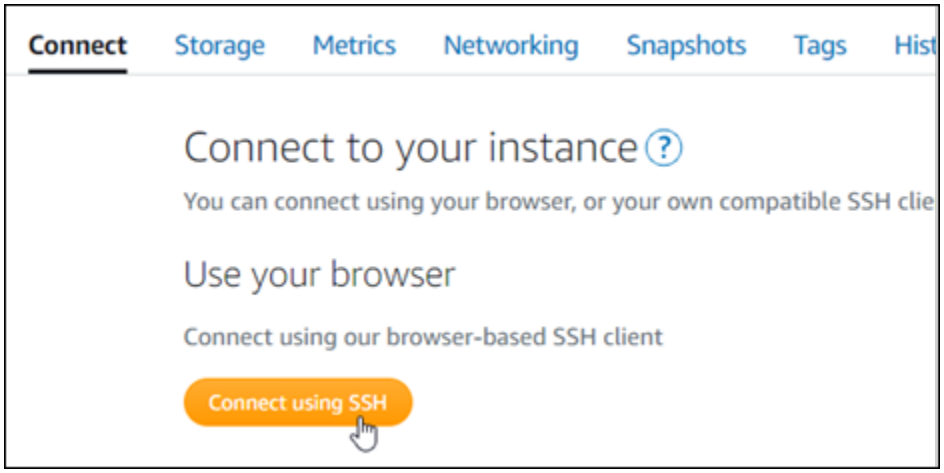
Schritt 4: Datenverkehr für Ihren registrierten Domänennamen auf Ihre Magento-Website weiterleiten

Um den Datenverkehr für Ihren registrierten Domänennamen, z. B. `example.com`, auf Ihrer Magento-Website weiterzuleiten, fügen Sie zum Domain Name System (DNS) Ihrer Domäne eine Akte hinzu. DNS-Datensätze werden in der Regel beim Registrar verwaltet und gehostet, bei dem Sie Ihre Domäne registriert haben. Wir empfehlen jedoch, die Verwaltung der DNS-Datensätze Ihrer Domäne auf Lightsail zu übertragen, damit Sie sie über die Lightsail-Konsole verwalten können.

Wählen Sie auf der Startseite der Lightsail-Konsole unter der Registerkarte Domains & DNS (Domains und DNS) die Option Create DNS zone (DNS-Zone erstellen) und folgen Sie dann den Anweisungen auf der Seite. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain in Lightsail.

Nachdem Ihr Domänenname Datenverkehr an Ihre Instance weitergeleitet hat, müssen Sie die folgenden Schritte ausführen, um die Magento-Software auf den Domänennamen aufmerksam zu machen.

1. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Verbinden die Option Verbinden mit SSH.



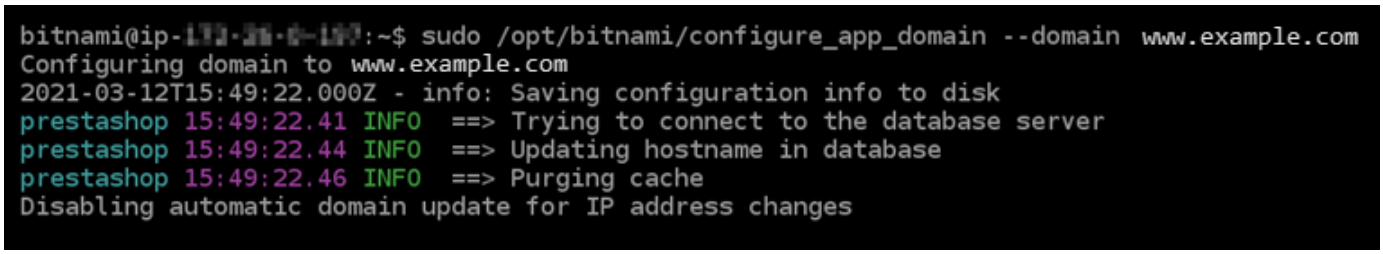
2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein. Stellen Sie sicher, dass Sie*<DomainName>*mit dem Domänennamen ersetzen, der Datenverkehr an Ihre Instance weiterleitet.

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

   Beispiel:

```
sudo /opt/bitnami/configure_app_domain --domain www.example.com
```

Sie sollten eine Reaktion ähnlich dem folgenden Beispiel erhalten. Die Magento-Software sollte nun den Domänennamen erkannt haben.

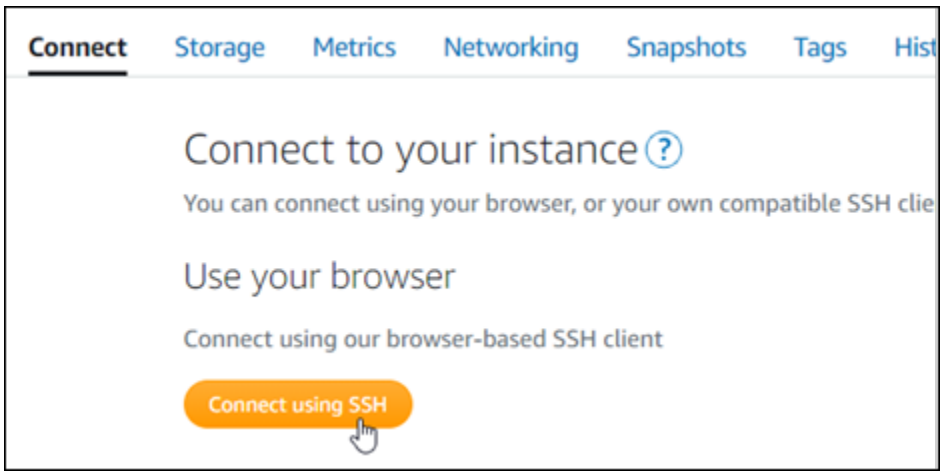


Schritt 5: HTTPS für Ihre Magento-Website konfigurieren

Führen Sie die folgenden Schritte aus, um HTTPS auf Ihrer Magento-Website zu konfigurieren. Diese Schritte zeigen, wie Sie das Bitnami HTTPS-Konfigurationstool (bncert) verwenden, welches ein Befehlszeilentool zum Anfordern von SSL/TLS-Zertifikaten, Einrichten von Umleitungen (z. B. HTTP zu HTTPS) und Erneuern von Zertifikaten ist.

> **Important**
>
> Das bncert-Tool stellt Zertifikate nur für Domänen aus, die derzeit Datenverkehr an die öffentliche IP-Adresse Ihrer Magento-Instance weiterleiten. Bevor Sie mit diesen Schritten beginnen, stellen Sie sicher, dass Sie DNS-Akten zum DNS aller Domänen hinzufügen, die Sie mit Ihrer Magento-Website verwenden möchten.

1. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Verbinden, die Option Verbinden mit SSH.



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um das bncert-tool zu starten.

```
sudo /opt/bitnami/bncert-tool
```

Sie sollten eine Reaktion ähnlich dem folgenden Beispiel erhalten:

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/bncert-tool
Warning: Custom redirections are not supported in the Bitnami Magento Stack.
This tool will not be able to enable/disable redirections.
Press [Enter] to continue:
```

3. Geben Sie Ihren primären Domänennamen und alternative Domänennamen durch ein Leerzeichen getrennt ein, wie im folgenden Beispiel gezeigt.

```
--------------------------------------------------------------------------------
Welcome to the Bitnami HTTPS Configuration tool.

--------------------------------------------------------------------------------
Domains

Please provide a valid space-separated list of domains for which you wish to
configure your web server.

Domain list []: example.com www.example.com
```

4. Die Änderungen, die vorgenommen werden, sind aufgelistet. Y eingeben undEingabe drücken, um zu bestätigen und fortzufahren.

```
------------------------------------------------------------------------
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
 example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

5. Geben Sie Ihre E-Mail-Adresse ein, die Sie Ihrem Let's-Encrypt-Zertifikat zuordnen möchten, und drücken SieEingabe.

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

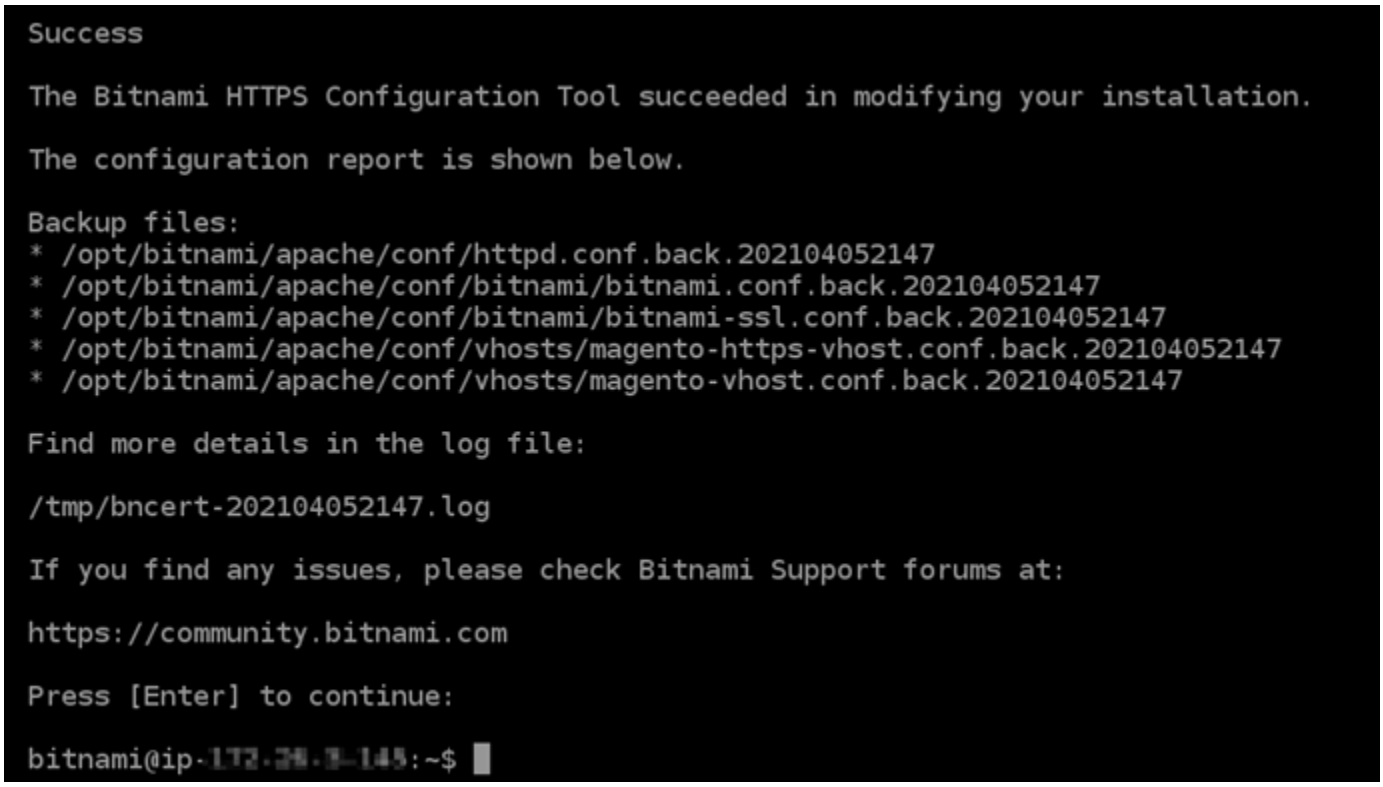
6. Lesen Sie die Let's-Encrypt-Subscriber-Vereinbarung. Y eingeben undEingabe drücken, um die Vereinbarung zu akzeptieren und fortzufahren.

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

Die Aktionen werden ausgeführt, um HTTPS für Ihre Instance zu aktivieren, einschließlich der Anforderung des Zertifikats und der Konfiguration der angegebenen Umleitungen.

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.

|
```

Ihr Zertifikat wurde erfolgreich ausgestellt und validiert, und die Umleitungen werden erfolgreich für Ihre Instance konfiguriert, wenn eine Meldung ähnlich dem folgenden Beispiel angezeigt wird.



Das `bncert`-Tool führt alle 80 Tage vor Ablauf Ihres Zertifikats eine automatische Erneuerung durch. Fahren Sie mit den nächsten Schritten fort, um die Aktivierung von HTTPS auf Ihrer Magento-Website abzuschließen.

7. Navigieren Sie zu der folgenden Adresse, um die Anmeldeseite für das Verwaltungs-Dashboard Ihrer Magento-Website aufzurufen. Stellen Sie sicher, dass Sie *<DomainName>* mit dem angemeldeten Domänennamen ersetzen, der Datenverkehr an Ihre Instance weiterleitet.

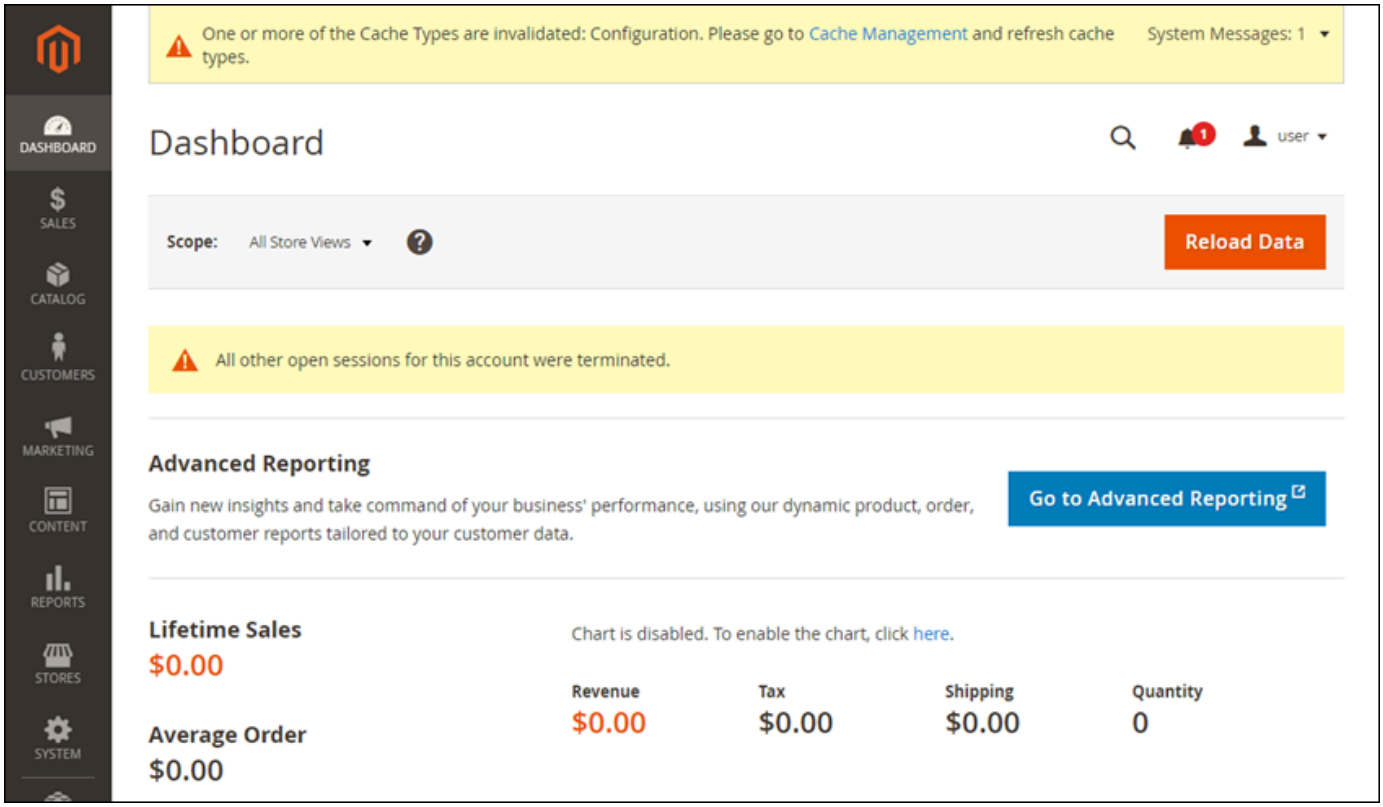
   ```
   http://<DomainName>/admin
   ```

   Beispiel:

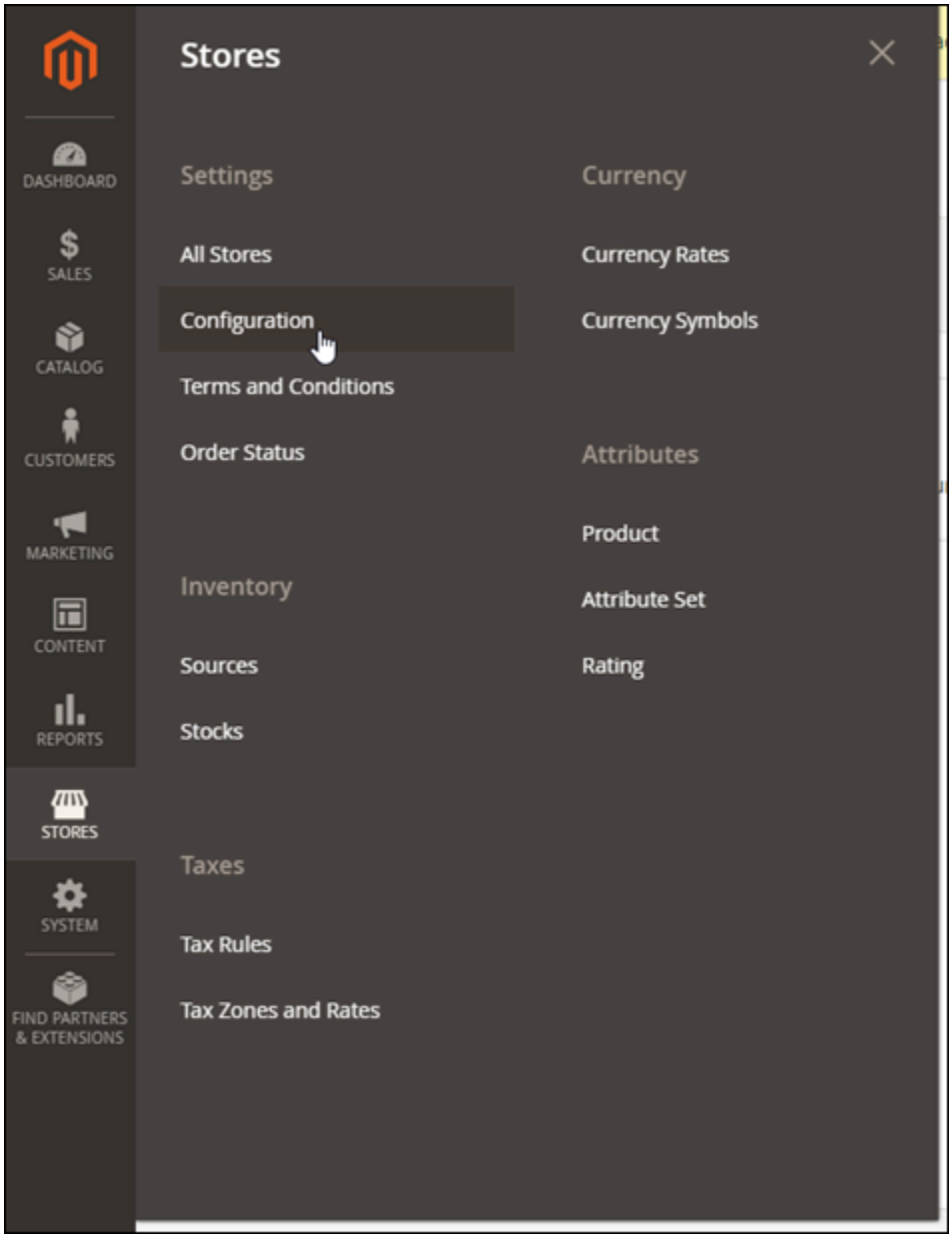
   ```
   http://www.example.com/admin
   ```

8. Geben Sie den Standard-Benutzernamen ein (`user`), das Standard-Anwendungspasswort, das Sie zuvor in diesem Leitfaden erhalten haben, und wählen Sie Sign in (Anmelden) aus.

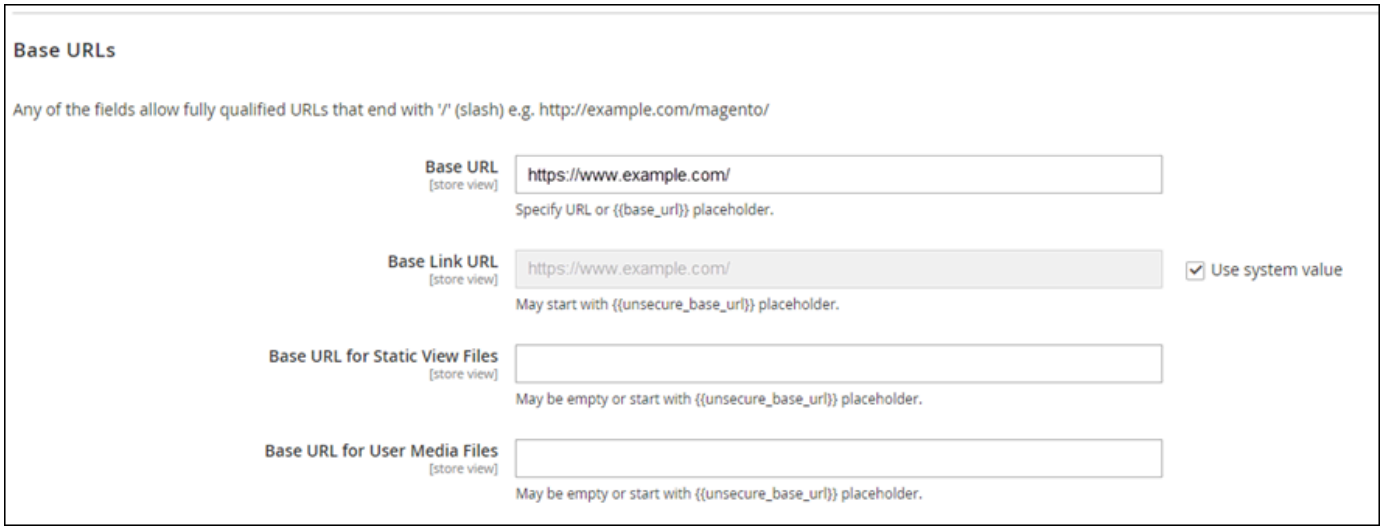
Das Magento-Verwaltungs-Dashboard wird angezeigt.



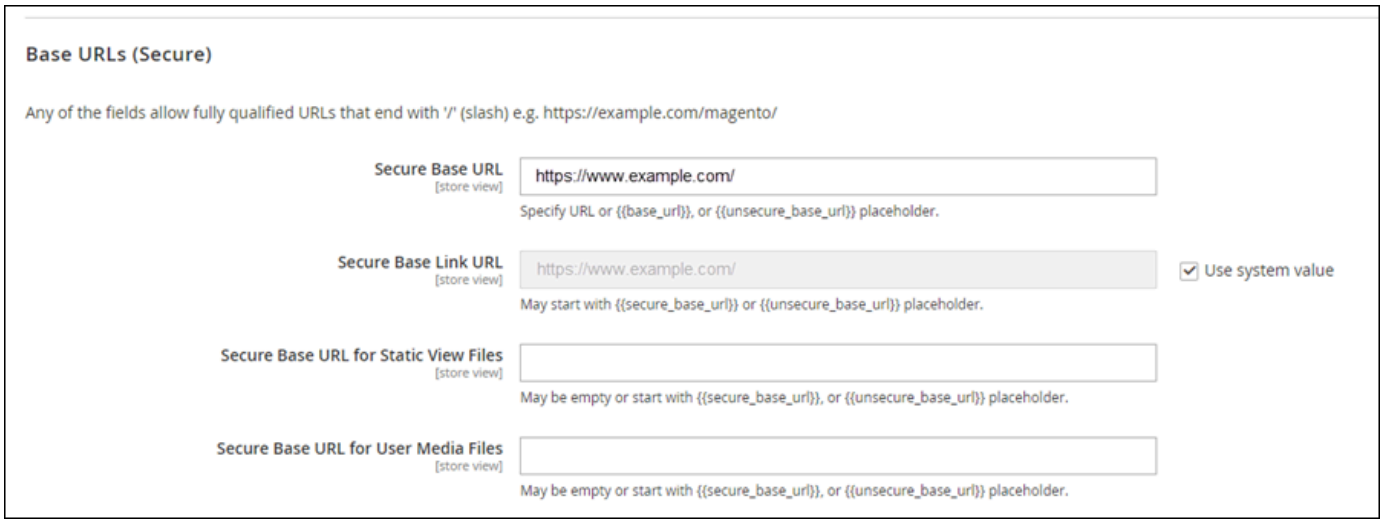
9. Wählen Sie im Navigationsbereich Stores (Speicher) und dann Configuration (Konfiguration) aus.



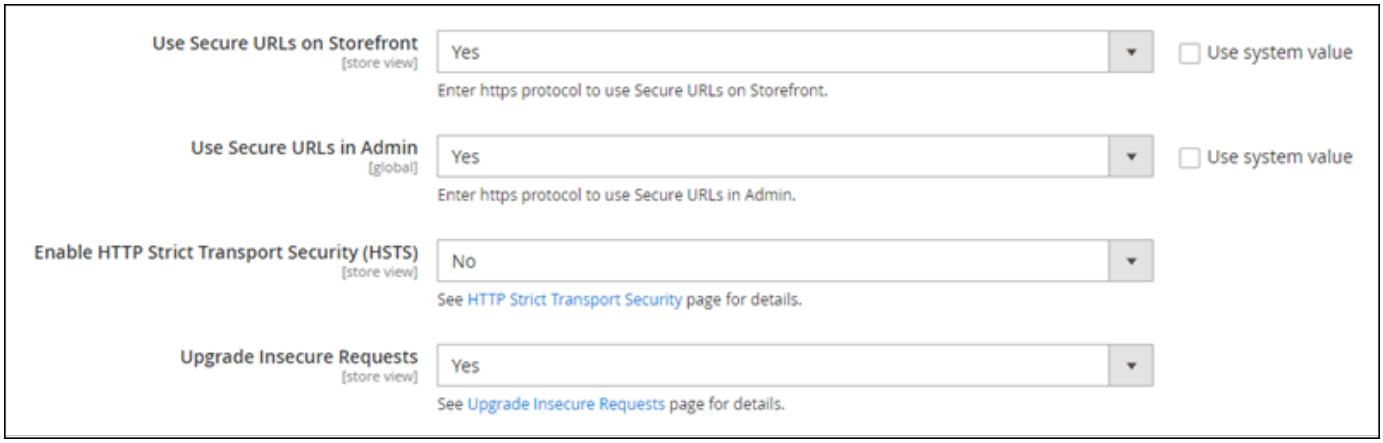
10. Klicken Sie auf Web und erweitern Sie dann den Basis-URLs-Knoten.
11. Geben Sie im Textfeld der Base URL (Basis-URL) die vollständige URL Ihrer Website ein, z. B. `https://www.example.com/`.



12. Erweitern Sie den (sicheren) Knoten der Basis-URLs.
13. Geben Sie im Textfeld Secure Base URL (Sichere Basis-URL) die vollständige URL Ihrer Website ein, z. B. `https://www.example.com/`.



14. Wählen Sie Yes (Ja) für die Optionen Use Secure URLs on Storefront (Sichere URLs auf Storefront verwenden), Use Secure URLs in Admin (Sichere URLs im Admin verwenden) und Upgrade Insecure Requests (Unsichere Anfragen aktualisieren).



15. Wählen Sie oben auf der Seite Konfiguration speichern aus.

    HTTPS ist jetzt für Ihre Magento-Website konfiguriert. Wenn Kunden zur HTTP-Version (z. B. `http://www.example.com`) Ihrer Magento-Website navigieren, werden diese automatisch auf die HTTPS-Version (z. B. `https://www.example.com`) umgeleitet.

Schritt 6: SMTP für E-Mail-Benachrichtigungen konfigurieren

Konfigurieren Sie die SMTP-Einstellungen Ihrer Magento-Website, um E-Mail-Benachrichtigungen dafür zu aktivieren. Weitere Informationen finden Sie unter Installieren der Magento-Magepal-SMTP-Erweiterung in der Bitnami-Dokumentation.

> **Important**
>
> Wenn Sie SMTP für die Verwendung der Ports 25, 465 oder 587 konfigurieren, dann müssen Sie diese Ports in der Firewall Ihrer Instance in derLightsail-Konsole öffnen. Weitere Informationen finden Sie unter Hinzufügen und Bearbeiten von Instance-Firewallregeln in Amazon Lightsail.
> Wenn Sie Ihr Gmail-Konto so konfigurieren, dass E-Mails auf Ihrer Magento-Website gesendet werden, müssen Sie anstelle des Standardpassworts, mit dem Sie sich bei Gmail anmelden, ein App-Passwort verwenden. Weitere Informationen finden Sie unter Anmelden mit App-Passwörtern.

Schritt 7: Die Bitnami- und Magento-Dokumentation lesen

Lesen Sie die Bitnami-Dokumentation, um zu erfahren, wie Sie verwaltende Aufgaben auf Ihrer Magento-Instance und Website durchführen können, wie z. B. Plug-Ins installieren und das Design

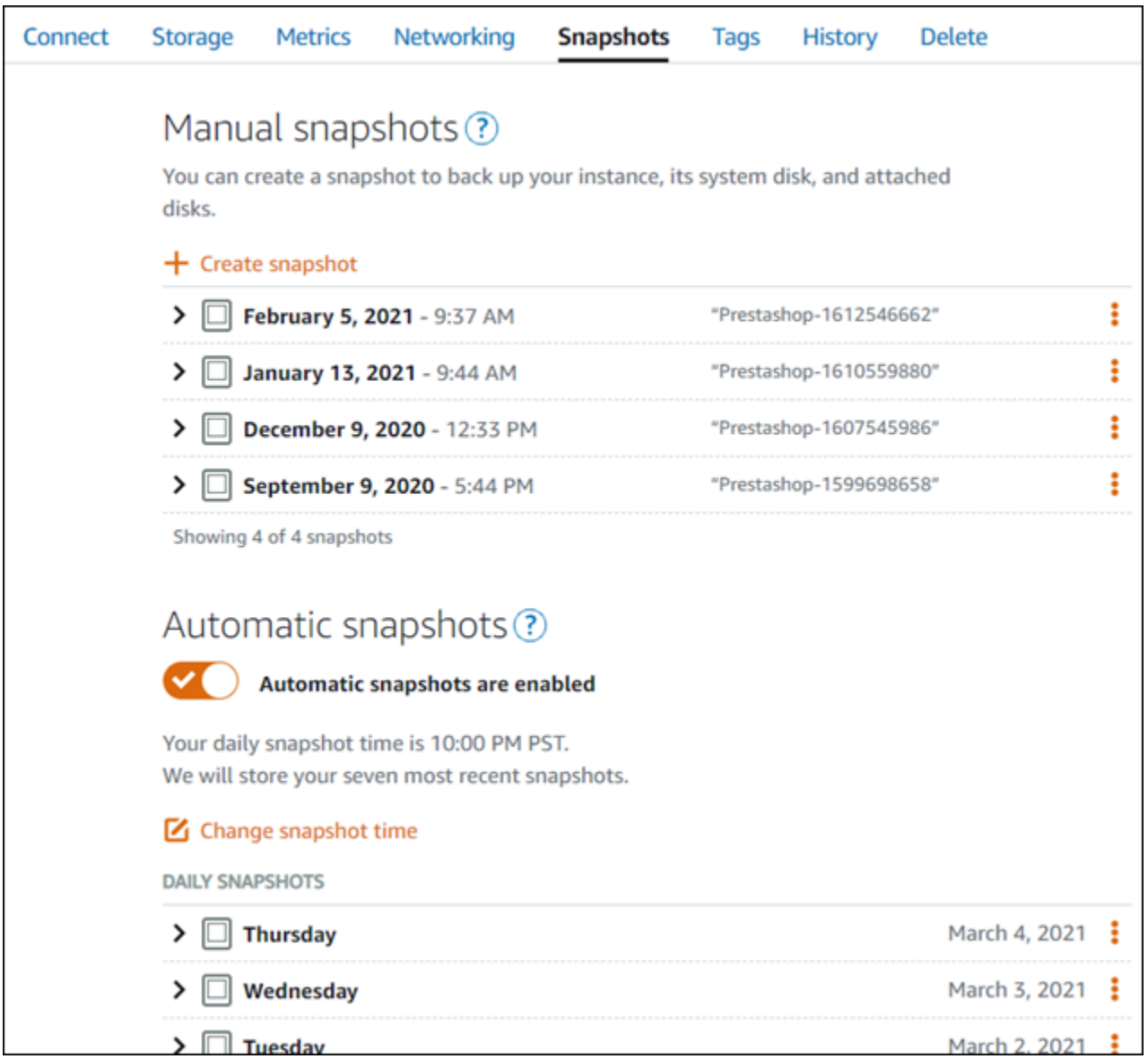
anpassen. Weitere Informationen finden Sie unter Bitnami-Magento-Stack For AWS Cloud in der Bitnami-Dokumentation.

Lesen Sie auch die Magento-Dokumentation, um zu erfahren, wie Sie Ihre Magento-Website verwalten. Weitere Informationen finden Sie im Magento-2.4-Benutzerhandbuch.

Schritt 8: Einen Snapshot Ihrer Magento-Instance erstellen

Nachdem Sie Ihre Magento-Website so konfiguriert haben, wie Sie sie möchten, erstellen Sie periodische Snapshots Ihrer Instance, um diese zu sichern. Sie können Snapshots manuell erstellen oder automatische Snapshots aktivieren, damit Lightsail tägliche Snapshots für Sie erstellt.. Wenn etwas mit Ihrer Instance nicht stimmt, können Sie mit dem Snapshot eine neue Ersatz-Instance erstellen. Weitere Informationen finden Sie unter Snapshots.

Wählen Sie auf der Instance-Verwaltungsseite, unter der RegisterkarteSnapshotSnapshot erstellenoder wählen Sie aus, automatische Snapshots zu aktivieren.



Weitere Informationen finden Sie unter Erstellen eines Snapshots IhrerLinux- oder Unix-Instance inAmazon LightsailoderAktivieren oder Deaktivieren von automatischen Snapshots für Instances oder Datenträger inAmazon Lightsail.

Schnellstartanleitung: Nginx

Hier sind einige erste Schritte, die Sie unternehmen sollten, nachdem Ihre Nginx-Instance auf Amazon Lightsail hochgefahren ist und läuft:

Schritt 1: Holen Sie sich das Standard-Anwendungspasswort für Ihre Nginx-Instance

Sie benötigen das Standard-Anwendungspasswort, um auf vorinstallierte Anwendungen oder Dienste auf Ihrer Instance zugreifen zu können.

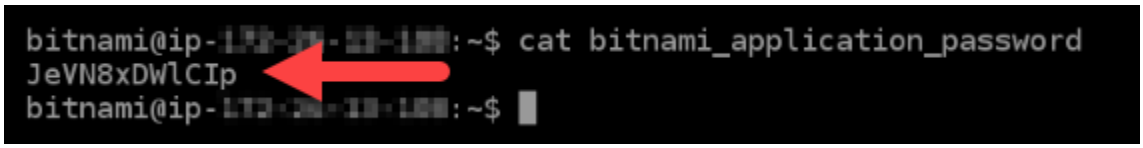
> **Important**
>
> Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um über IPv6 SSH oder RDP in Ihre Instance zu senden. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).
2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um das Standard-Anwendungspasswort zu erhalten:

   ```
   cat bitnami_application_password
   ```

   > **Note**
   >
   > Wenn Sie sich in einem anderen Verzeichnis als dem Stammverzeichnis des Benutzers befinden, geben Sie `cat $HOME/bitnami_application_password` ein.

   Sie sollten eine ähnliche Antwort wie diese sehen, die das Standard-Anwendungspasswort enthält:

Weitere Informationen finden Sie unter Abrufen des Anwendungsbenutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.

Schritt 2: Fügen Sie an Ihre Nginx-Instance eine statische IP-Adresse an

Die standardmäßig an Ihre Instance angefügte dynamische öffentliche IP-Adresse ändert sich bei jedem Stopp und Start der Instance. Erstellen Sie eine statische IP-Adresse und fügen Sie sie an Ihre Instance an, damit die öffentliche IP-Adresse nicht mehr geändert wird. Später, wenn Sie Ihren Domainnamen mit Ihrer Instance verwenden, müssen Sie die DNS-Datensätze Ihrer Domain nicht jedes Mal aktualisieren, wenn Sie die Instance stoppen und starten. Sie können eine statische IP an eine Instance anhängen.

Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Domains & DNS (Domains und DNS) die Option Create static IP (Statische IP erstellen) und folgen Sie dann den Anweisungen auf der Seite.

Weitere Informationen finden Sie unter Erstellen einer statischen IP und Anfügen an eine Instance in Lightsail.

Schritt 3: Besuchen Sie die Startseite Ihrer Nginx-Instance

Navigieren Sie zur öffentlichen IP-Adresse Ihrer Instance, um auf die darauf installierte Anwendung zuzugreifen phpMyAdmin, auf zuzugreifen oder auf die Bitnami-Dokumentation zuzugreifen.

1. Notieren Sie sich von Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die öffentliche IP-Adresse.
2. Navigieren Sie zur öffentlichen IP-Adresse, indem Sie z. B. zu `http://192.0.2.3` gehen.

Weitere Informationen finden Sie unter Abrufen des Anwendungsbenutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.

Schritt 4: Ordnen Sie Ihren Domänennamen Ihrer Nginx-Instance zu

Um Ihren Domänennamen, wie z. B. `example.com`, auf Ihre Instance abzubilden, fügen Sie einen Datensatz zum Domain Name System (DNS) Ihrer Domäne hinzu. DNS-Datensätze werden in der Regel beim Registrar verwaltet und gehostet, bei dem Sie Ihre Domain registriert haben. Wir empfehlen jedoch, die Verwaltung der DNS-Datensätze Ihrer Domain an Lightsail zu übertragen, damit Sie sie mit der Lightsail-Konsole verwalten können.

Wählen Sie auf der Startseite der Lightsail-Konsole auf der Registerkarte Netzwerk die Option DNS-Zone erstellen aus und folgen Sie dann den Anweisungen auf der Seite.

Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.

Schritt 5: Lesen Sie die Bitnami-Dokumentation

Lesen Sie die Bitnami-Dokumentation, um zu erfahren, wie Sie Ihre Nginx-Anwendung bereitstellen, die HTTPS-Unterstützung mit SSL-Zertifikaten aktivieren, Dateien mit SFTP auf den Server hochladen und vieles mehr.

Weitere Informationen finden Sie unter Bitnami Nginx für die AWS Cloud.

Schritt 6: Erstellen Sie einen Snapshot Ihrer Nginx-Instance

Ein Snapshot ist eine Kopie des Systemlaufwerks und der ursprünglichen Konfiguration einer Instance. Der Snapshot enthält Informationen wie Speicher, CPU, Festplattengröße und Datenübertragungsrate. Sie können einen Snapshot als Grundlage für neue Instances oder als Datensicherung verwenden.

Geben Sie auf Ihrer Instance-Verwaltungsseite auf der Registerkarte Snapshot einen Namen für den Snapshot ein und wählen Sie dann Create snapshot (Snapshot erstellen) aus.

Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Linux- oder Unix-Instance.

Schnellstartanleitung: Node.js

Hier finden Sie einige erste Schritte, die Sie unternehmen sollten, nachdem Ihre Node.js-Instance auf Amazon Lightsail hochgefahren ist und läuft:

Schritt 1: Holen Sie sich das Standard-Anwendungspasswort für Ihre Node.js-Instance

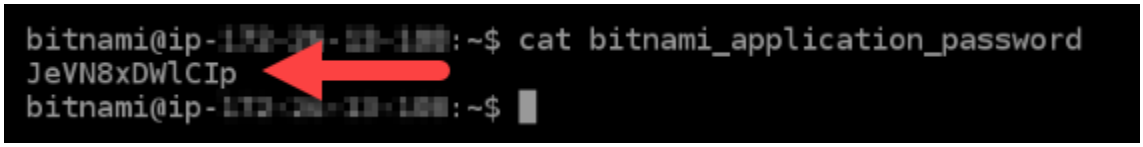
Sie benötigen das Standard-Anwendungspasswort, um auf vorinstallierte Anwendungen oder Dienste auf Ihrer Instance zugreifen zu können.

1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).
2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um das Standard-Anwendungspasswort zu erhalten:

```
cat bitnami_application_password
```

> **Note**
>
> Wenn Sie sich in einem anderen Verzeichnis als dem Stammverzeichnis des Benutzers befinden, geben Sie `cat $HOME/bitnami_application_password` ein.

Sie sollten eine ähnliche Antwort wie diese sehen, die das Standard-Anwendungspasswort enthält:



Weitere Informationen finden Sie unter Abrufen des Anwendungs-Benutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.

Schritt 2: Fügen Sie an Ihre Node.js-Instance eine statische IP-Adresse an

Die standardmäßig an Ihre Instance angefügte dynamische öffentliche IP-Adresse ändert sich bei jedem Stopp und Start der Instance. Erstellen Sie eine statische IP-Adresse und fügen Sie sie an Ihre Instance an, damit die öffentliche IP-Adresse nicht mehr geändert wird. Später, wenn Sie Ihren Domänennamen mit Ihrer Instance verwenden, müssen Sie die DNS-Datensätze Ihrer Domäne nicht jedes Mal aktualisieren, wenn Sie die Instance stoppen und starten. Sie können eine statische IP an eine Instance anhängen.

Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Domains & DNS (Domains und DNS) die Option Create static IP (Statische IP erstellen) und folgen Sie dann den Anweisungen auf der Seite.

Weitere Informationen finden Sie unter Erstellen Sie eine statische IP-Adresse und fügen Sie sie an eine Instance in Lightsail an.

Schritt 3: Besuchen Sie die Startseite Ihrer Node.js-Instance

Navigieren Sie zur öffentlichen IP-Adresse Ihrer Instance, um auf die darauf installierte Anwendung zuzugreifen, auf phpMyAdmin oder auf die Bitnami-Dokumentation.

1. Notieren Sie sich von Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die öffentliche IP-Adresse.

2. Navigieren Sie zur öffentlichen IP-Adresse, indem Sie z. B. zu `http://192.0.2.3` gehen.

Weitere Informationen finden Sie unter Abrufen des Anwendungs-Benutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.

Schritt 4: Ordnen Sie Ihren Domänennamen Ihrer Node.js-Instance zu

Um Ihren Domänennamen, wie z. B. `example.com`, auf Ihre Instance abzubilden, fügen Sie einen Datensatz zum Domain Name System (DNS) Ihrer Domäne hinzu. DNS-Datensätze werden in der Regel beim Registrar verwaltet und gehostet, bei dem Sie Ihre Domäne registriert haben. Wir empfehlen jedoch, die Verwaltung der DNS-Datensätze Ihrer Domäne auf Lightsail zu übertragen, damit Sie sie über die Lightsail-Konsole verwalten können.

Wählen Sie auf der Startseite der Lightsail-Konsole unter der Registerkarte Networking (Netzwerk) die Option Create DNS zone (DNS-Zone erstellen) und folgen Sie dann den Anweisungen auf der Seite.

Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.

Schritt 5: Lesen Sie die Bitnami-Dokumentation

Lesen Sie die Bitnami-Dokumentation, um zu erfahren, wie Sie Ihre Node.js-Anwendung bereitstellen, die HTTPS-Unterstützung mit SSL-Zertifikaten aktivieren, Dateien mit SFTP auf den Server hochladen und vieles mehr.

Weitere Informationen finden Sie unter Bitnami Node.js für die AWS Cloud.

Schritt 6: Erstellen Sie einen Snapshot Ihrer Node.js-Instance

Ein Snapshot ist eine Kopie des Systemlaufwerks und der ursprünglichen Konfiguration einer Instance. Der Snapshot enthält Informationen wie Speicher, CPU, Festplattengröße und Datenübertragungsrate. Sie können einen Snapshot als Grundlage für neue Instances oder als Datensicherung verwenden.

Geben Sie auf Ihrer Instance-Verwaltungsseite auf der Registerkarte Snapshot einen Namen für den Snapshot ein und wählen Sie dann Create snapshot (Snapshot erstellen) aus.

Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Linux- oder Unix-Instance.

Schnellstartanleitung: Plesk

Hier sind einige erste Schritte, die Sie unternehmen sollten, nachdem Ihre Plesk-Instance auf Amazon Lightsail hochgefahren ist und läuft:

> **Important**
>
> Wenn nach dem Start Ihrer Plesk-Instance Probleme auftreten, rufen Sie die Plesk-Supportseite auf, um zu sehen, ob Updates auf der Instance installiert werden müssen. Weitere Informationen finden Sie im Plesk-Hilfecenter und Plesk-Updates im Plesk-Dokumentations- und Hilfeportal.

Schritt 1: Abruf der einmaligen Anmelde-URL für Ihre Plesk-Instance

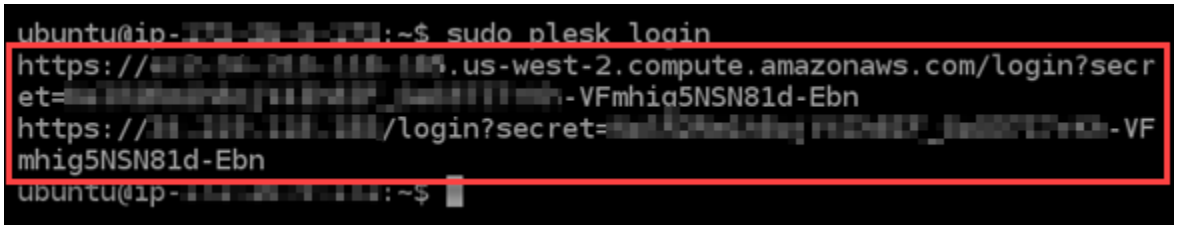
Sie benötigen die einmalige Anmelde-URL für den Zugriff auf das Plesk-Panel als Administrator.

> **Important**
>
> Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um über IPv6 SSH oder RDP in Ihre Instance zu senden. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).
2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um die einmalige Anmelde-URL zu erhalten:

   ```
   sudo plesk login | grep -v internal:8
   ```

   Ihnen sollten eine Antwort ähnlich der folgenden mit einer einmaligen Anmelde-URL angezeigt werden:



> **Important**
>
> Wenn Sie kürzlich eine statische IP an Ihre Plesk-Instance angehängt haben, erhalten Sie möglicherweise eine einmalige Anmelde-URL, die die alte öffentliche IP-Adresse verwendet. Starten Sie die Instance neu und führen Sie dann den obigen Befehl erneut aus, um eine einmalige Anmelde-URL zu erhalten, die die neue statische, öffentliche IP-Adresse verwendet.

3. Kopieren Sie die URL in die Zwischenablage, oder notieren Sie sie. Sie benötigen sie später für die erstmalige Anmeldung im Plesk-Panel.

Weitere Informationen finden Sie unter Einrichten und Konfigurieren von Plesk auf Lightsail.

Schritt 2: Erste Anmeldung beim Plesk-Panel

Fügen Sie die einmalige Anmelde-URL in einem Web-Browser ein. Folgen Sie den Anweisungen auf der Seite, um Ihre Anmeldeinformationen für Plesk zu erstellen. Bei der ersten Anmeldung sollte Ihnen eine Option zum Hinzufügen Ihrer Domain zu Plesk angezeigt werden.

> **Note**
>
> Möglicherweise warnt Ihr Browser Sie davor, dass Ihre Verbindung nicht privat bzw. sicher ist oder dass ein Sicherheitsrisiko besteht. Dies geschieht, weil Ihre Plesk-Instance noch nicht über eine SSL/TLS-Zertifikat verfügt. Wählen Sie im Browserfenster Advanced (Erweitert) und dann Details oder More information (Weitere Informationen), um die verfügbaren Optionen anzuzeigen. Besuchen Sie dann die Website, auch wenn diese nicht privat oder sicher ist.

Weitere Informationen finden Sie unter Einrichten und Konfigurieren von Plesk auf Lightsail.

Schritt 3: Anfügen einer statischen IP-Adresse an Ihre Plesk-Instance

Die standardmäßig an Ihre Instance angefügte dynamische öffentliche IP-Adresse ändert sich bei jedem Stopp und Start der Instance. Erstellen Sie eine statische IP-Adresse und fügen Sie sie an Ihre Instance an, damit die öffentliche IP-Adresse nicht mehr geändert wird. Später, wenn Sie Ihren Domainnamen mit Ihrer Instance verwenden, müssen Sie die DNS-Datensätze Ihrer Domain nicht jedes Mal aktualisieren, wenn Sie die Instance stoppen und starten. Sie können eine statische IP an eine Instance anhängen.

Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Networking (Netzwerk) die Option Create static IP (Statische IP erstellen) und folgen Sie dann den Anweisungen auf der Seite.

Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

Schritt 4: Zuordnen Ihres Domänennamens zu Ihrer Plesk-Instance

> **Note**
>
> Sie können Ihrer Plesk-Instance eine Domain zuordnen, mit der Sie auf Ihren Plesk-Bereich zugreifen können. Sie können auch mehrere Domains innerhalb des Plesk-Bereichs zuordnen, die Sie zur Verwaltung von Websites innerhalb des Plesk-Bereichs verwenden können. In diesem Abschnitt wird beschrieben, wie Sie Ihre Domain Ihrer Plesk-Instance zuordnen. Weitere Informationen zum Zuordnen mehrerer Domains im Plesk-Bereich finden Sie unter Hinzufügen einer Domain in Plesk im Plesk Documentation and Help Portal.

Um Ihren Domänennamen, wie z. B. `example.com`, auf Ihre Instance abzubilden, fügen Sie einen Datensatz zum Domain Name System (DNS) Ihrer Domäne hinzu. DNS-Datensätze werden in der Regel beim Registrar verwaltet und gehostet, bei dem Sie Ihre Domain registriert haben. Wir empfehlen jedoch, die Verwaltung der DNS-Datensätze Ihrer Domain auf Lightsail zu übertragen, damit Sie sie über die Lightsail-Konsole verwalten können.

Wählen Sie auf der Startseite der Lightsail-Konsole auf der Registerkarte Domains und DNS die Option DNS-Zone erstellen aus und folgen Sie dann den Anweisungen auf der Seite.

Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain in Lightsail.

Schritt 5: Lesen Sie die Plesk-Dokumentation

Lesen Sie die Plesk-Dokumentation, um zu erfahren, wie Sie Websites mit Plesk verwalten, das Plesk-Panel anpassen und vieles mehr.

Weitere Informationen finden Sie unter Erste Schritte mit der Verwaltung von Websites in Plesk im Plesk Documentation and Help Portal.

Schritt 6: Erstellen Sie einen Snapshot Ihrer Plesk-Instance

Ein Snapshot ist eine Kopie des Systemlaufwerks und der ursprünglichen Konfiguration einer Instance. Der Snapshot enthält Informationen wie Speicher, CPU, Festplattengröße und Datenübertragungsrate. Sie können einen Snapshot als Grundlage für neue Instances oder als Datensicherung verwenden.

Geben Sie auf Ihrer Instance-Verwaltungsseite auf der Registerkarte Snapshot einen Namen für den Snapshot ein und wählen Sie dann Create snapshot (Snapshot erstellen) aus.

Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Linux- oder Unix-Instance.

Schnellstartanleitung: PrestaShop

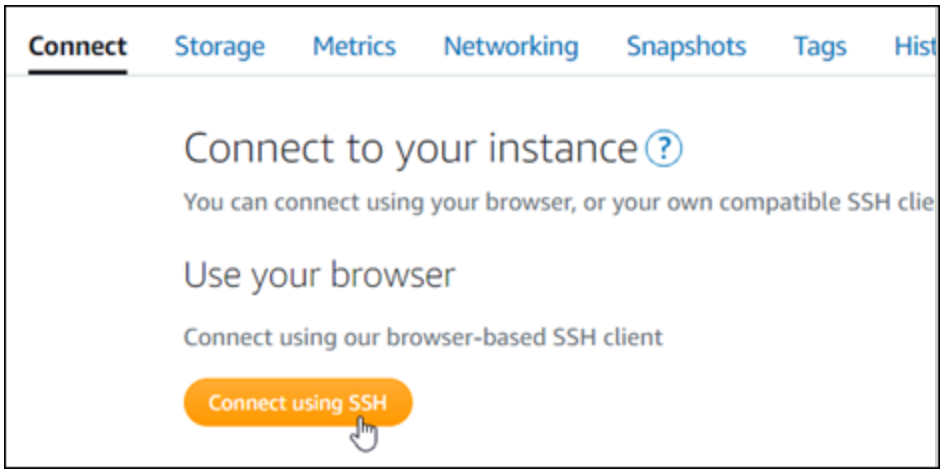
Hier sind einige Schritte, die Sie ausführen sollten, um loszulegen, nachdem Ihre PrestaShop Instance auf Amazon Lightsail betriebsbereit ist.

Inhalt

Schritt 1: Holen Sie sich das Standardanwendungskennwort für Ihre PrestaShop Website

Führen Sie die folgenden Schritte aus, um das Standardanwendungskennwort für Ihre PrestaShop Website zu erhalten.

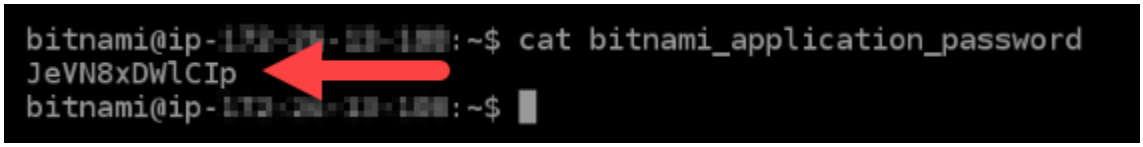
1. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Verbinden die Option Verbinden mit SSH.



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um das Standard-Anwendungspasswort zu erhalten:

```
cat $HOME/bitnami_application_password
```

Sie sollten eine ähnliche Antwort wie diese sehen, die das Standard-Anwendungspasswort enthält. Speichern Sie dieses Passwort an einem sicheren Ort. Sie werden es im nächsten Abschnitt dieses Tutorials verwenden, um sich im Administrations-Dashboard Ihrer Website anzumelden. PrestaShop



Weitere Informationen finden Sie unter Abrufen des Anwendungsbenutzernamens und des Kennworts für Ihre Bitnami-Instance in Amazon Lightsail.

Schritt 2: Hängen Sie eine statische IP-Adresse an Ihre Instance an PrestaShop

Die Ihrer Instance beim ersten Erstellen zugewiesene öffentliche IP-Adresse ändert sich bei jedem Stopp und Start Ihrer Instance. Sie sollten eine statische IP-Adresse erstellen und an Ihre Instance anfügen, um sicherzustellen, dass sich deren öffentliche IP-Adresse nicht ändert. Wenn Sie Ihrer Instance später einen registrierten Domänennamen wie zum Beispiel `example.com` zuweisen, müssen Sie nicht jedes Mal, wenn Sie Ihre Instance stoppen und neu starten, die DNS-Akte Ihrer Domäne aktualisieren. Sie können eine statische IP an eine Instance anhängen.

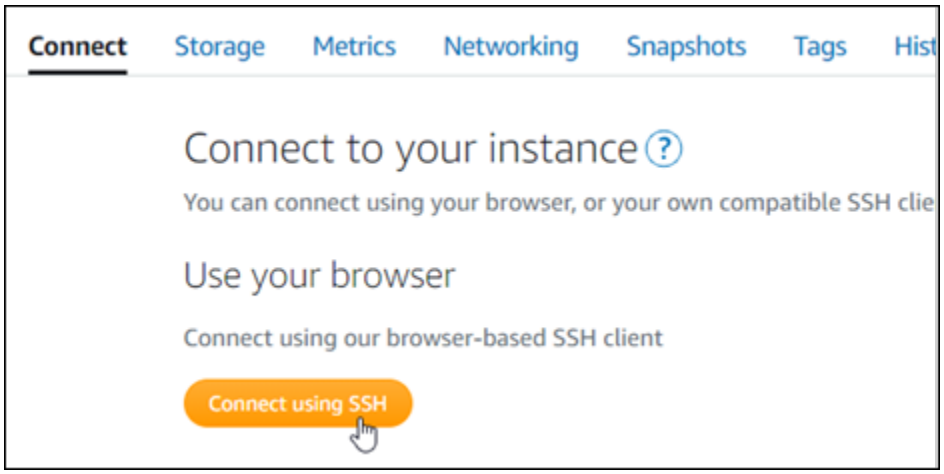
Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Netzwerk, die Registerkarte Erstellen einer statischen IP oder Anfügen einer statischen IP (falls Sie zuvor eine statische IP-Adresse erstellt haben, die Sie Ihrer Instance anfügen können) und folgen Sie dann den Anweisungen auf der Seite.

Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

Nachdem die neue statische IP-Adresse an Ihre Instance angehängt wurde, müssen Sie die folgenden Schritte ausführen, damit die PrestaShop Software auf die neue statische IP-Adresse aufmerksam wird.

1. Notieren Sie sich die statische IP-Adresse Ihrer Instance. Sie wird im Kopfzeilenabschnitt Ihrer Instance-Verwaltungsseite aufgeführt.

2. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Verbinden die Option Verbinden mit SSH.



3. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein. Stellen Sie sicher, dass Sie*<StaticIP>* mit der neuen statischen IP-Adresse Ihrer Instance ersetzen.

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

Beispiel:

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

Sie sollten eine Antwort ähnlich dem folgenden Beispiel erhalten. Die PrestaShop Software sollte jetzt die neue statische IP-Adresse kennen.

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

> **Note**
>
> PrestaShop unterstützt derzeit keine IPv6-Adressen. Sie können IPv6 für die Instance aktivieren, aber die PrestaShop Software reagiert nicht auf Anfragen über das IPv6-Netzwerk.

Schritt 3: Melden Sie sich im Administrations-Dashboard Ihrer Website an PrestaShop

Führen Sie den folgenden Schritt aus, um auf Ihre PrestaShop Website zuzugreifen und sich im Verwaltungs-Dashboard anzumelden. Um sich anzumelden, verwenden Sie den Standard-Benutzernamen (`user@example.com`) und das Standard-Anwendungspasswort, das Sie zuvor in diesem Leitfaden erhalten haben.

1. Notieren Sie sich in der Lightsail-Konsole die öffentliche oder statische IP-Adresse, die im Header-Bereich der Instanzverwaltungsseite aufgeführt ist.

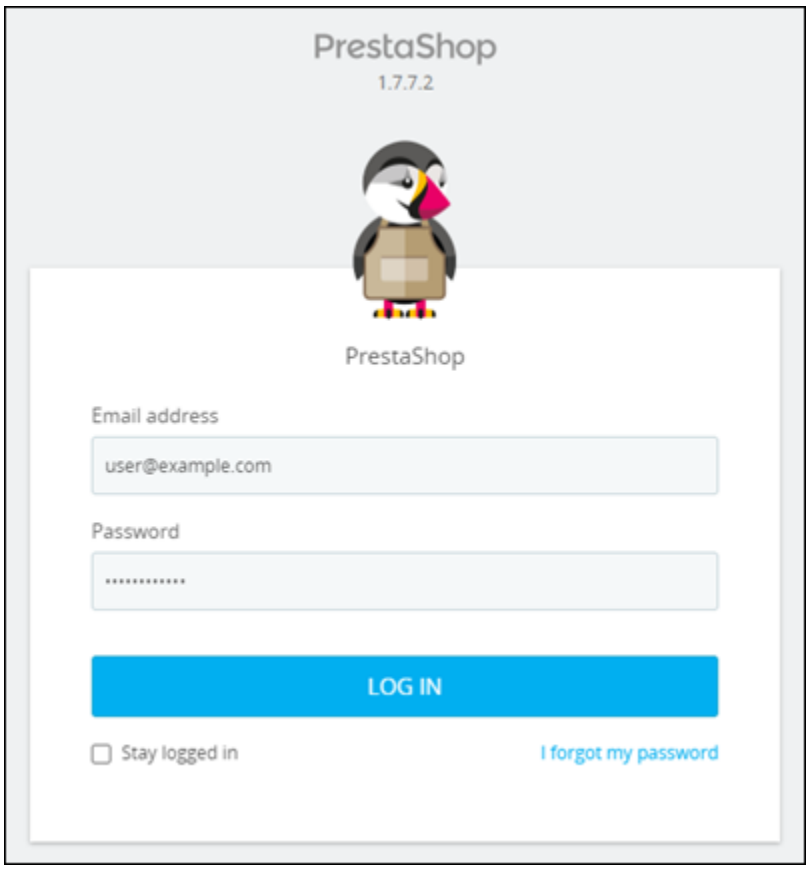
2. Rufen Sie die folgende Adresse auf, um auf die Anmeldeseite für das Administrations-Dashboard Ihrer PrestaShop Website zuzugreifen. Achten Sie darauf, *< InstanceIpAddress >* durch die öffentliche oder statische IP-Adresse Ihrer Instanz zu ersetzen.

```
http://<InstanceIpAddress>/administration
```

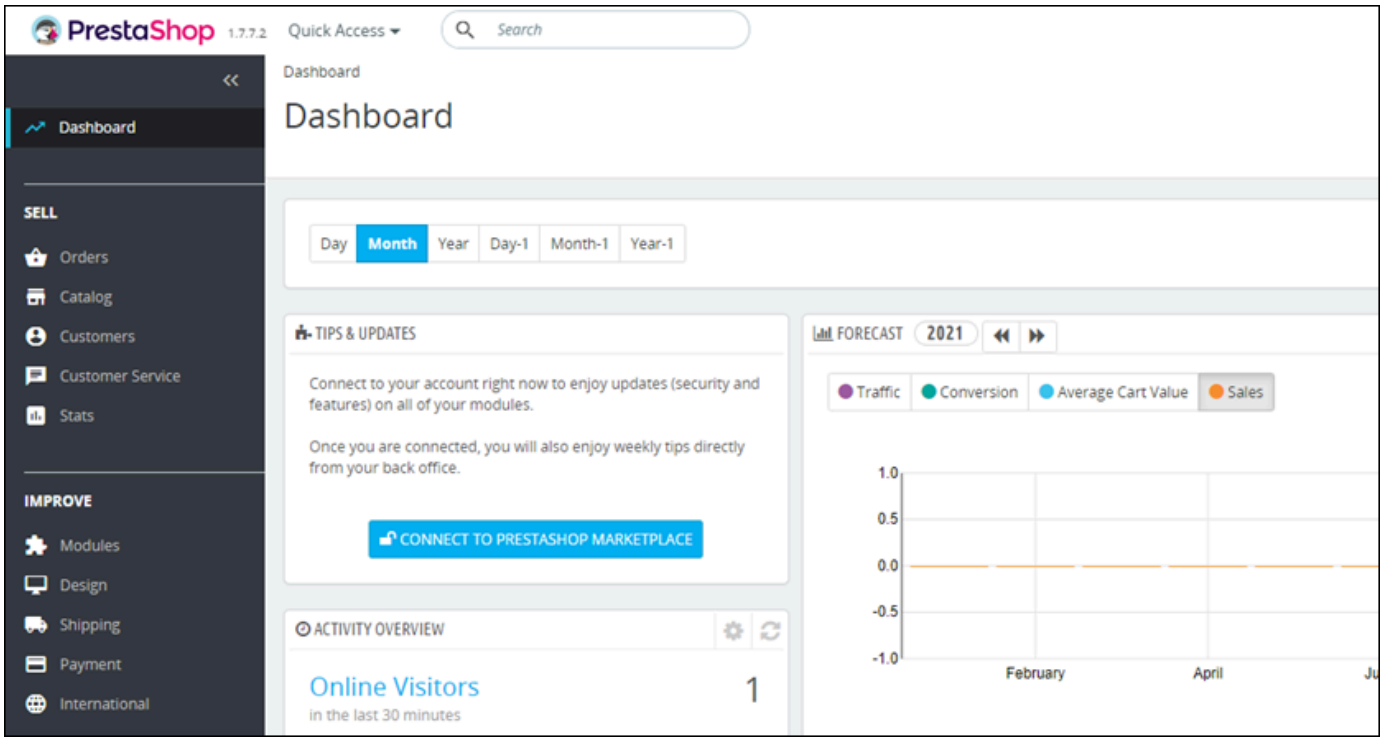
   Beispiel:

```
http://203.0.113.0/administration
```

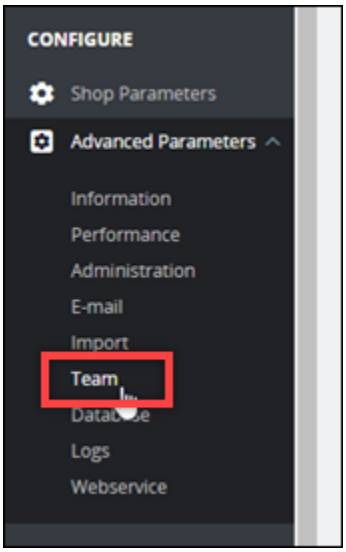
3. Geben Sie den Standard-Benutzernamen ein (`user@example.com`), das Standard-Anwendungspasswort, das Sie zuvor in diesem Leitfaden erhalten haben, und wählen Sie Anmelden aus.



Das PrestaShop Verwaltungs-Dashboard wird angezeigt.



Um den Standardbenutzernamen oder das Standardkennwort zu ändern, mit dem Sie sich im Verwaltungs-Dashboard Ihrer PrestaShop Website anmelden, wählen Sie im Navigationsbereich Erweiterte Parameter und dann Team aus. Weitere Informationen finden Sie PrestaShop im Benutzerhandbuch in der PrestaShop Dokumentation.



Weitere Informationen zum Administrations-Dashboard finden Sie unter Weitere Informationen finden Sie PrestaShop im Benutzerhandbuch in der PrestaShop Dokumentation.

Schritt 4: Leiten Sie den Traffic für Ihren registrierten Domainnamen auf Ihre PrestaShop Website weiter

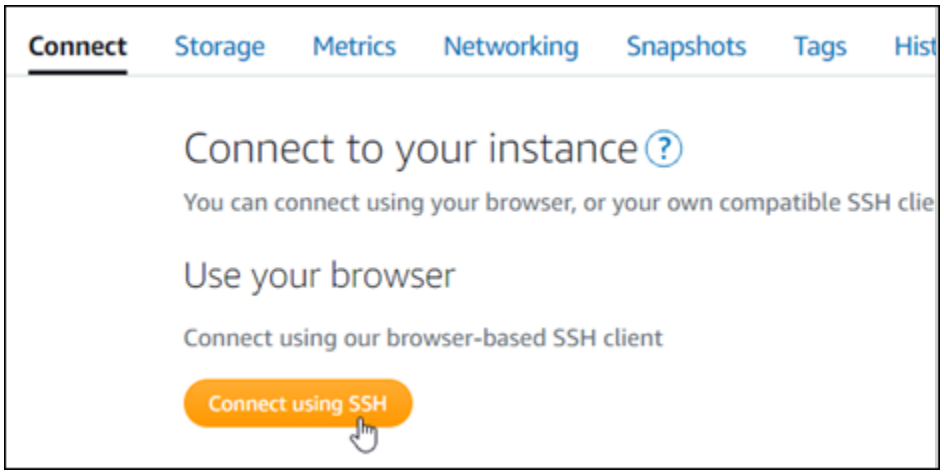
Um den Traffic für Ihren registrierten Domainnamen weiterzuleiten`example.com`, z. B. auf Ihre PrestaShop Website, fügen Sie dem Domainnamensystem (DNS) Ihrer Domain einen Eintrag hinzu. DNS-Datensätze werden in der Regel beim Registrar verwaltet und gehostet, bei dem Sie Ihre Domain registriert haben. Wir empfehlen Ihnen jedoch, die Verwaltung der DNS-Einträge Ihrer Domain an Lightsail zu übertragen, damit Sie sie über die Lightsail-Konsole verwalten können.

Wählen Sie auf der Startseite der Lightsail-Konsole unter dem Tab Domains & DNS die Option Create DNS zone aus und folgen Sie dann den Anweisungen auf der Seite.

Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Einträge Ihrer Domain in Lightsail.

Nachdem Ihr Domainname den Datenverkehr an Ihre Instance weitergeleitet hat, müssen Sie die folgenden Schritte ausführen, damit die PrestaShop Software den Domainnamen erkennt.

1. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Verbinden die Option Verbinden mit SSH.



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein. Achten Sie darauf, *< DomainName >* durch den Domainnamen zu ersetzen, der den Datenverkehr zu Ihrer Instance weiterleitet.

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

Beispiel:

```
sudo /opt/bitnami/configure_app_domain --domain www.example.com
```

Sie sollten eine Antwort ähnlich dem folgenden Beispiel erhalten. Die PrestaShop Software sollte jetzt den Domainnamen kennen.

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain www.example.com
Configuring domain to www.example.com
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

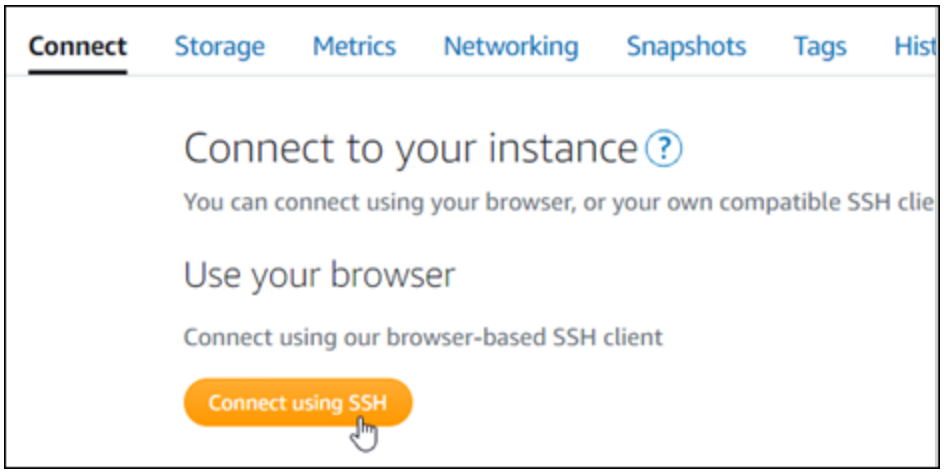
Schritt 5: Konfigurieren Sie HTTPS für Ihre PrestaShop Website

Gehen Sie wie folgt vor, um HTTPS auf Ihrer PrestaShop Website zu konfigurieren. Diese Schritte zeigen, wie Sie das Bitnami HTTPS-Konfigurationstool (bncert) verwenden, welches ein

Befehlszeilentool zum Anfordern von SSL/TLS-Zertifikaten, Einrichten von Umleitungen (z. B. HTTP zu HTTPS) und Erneuern von Zertifikaten ist.

> **Important**
>
> Das bncert-Tool stellt Zertifikate nur für Domains aus, die derzeit Datenverkehr an die öffentliche IP-Adresse Ihrer PrestaShop Instance weiterleiten. Bevor Sie mit diesen Schritten beginnen, stellen Sie sicher, dass Sie DNS-Einträge zum DNS aller Domains hinzufügen, die Sie mit Ihrer PrestaShop Website verwenden möchten.

1. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Verbinden, die Option Verbinden mit SSH.



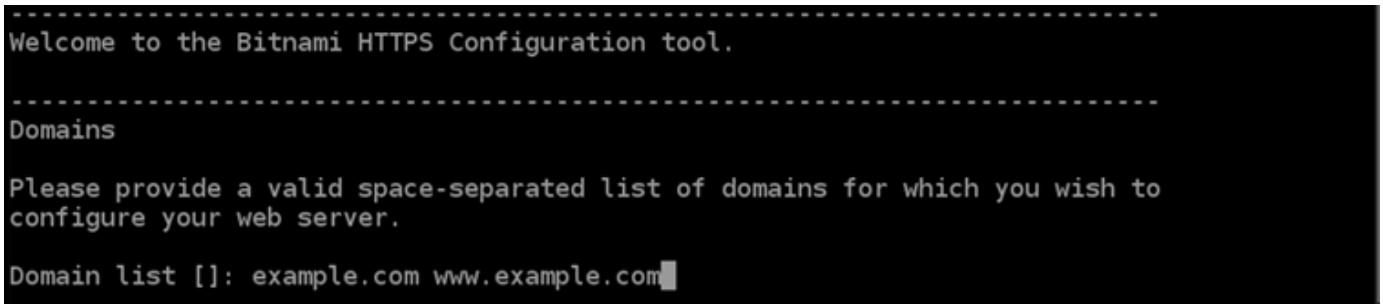
2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um das bncert-tool zu starten.

```
sudo /opt/bitnami/bncert-tool
```

Sie sollten eine Reaktion ähnlich dem folgenden Beispiel erhalten:

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/bncert-tool
--------------------------------------------------------------------------------
Welcome to the Bitnami HTTPS Configuration tool.

--------------------------------------------------------------------------------
Domains

Please provide a valid space-separated list of domains for which you wish to
configure your web server.

Domain list []:
```

3. Geben Sie Ihren primären Domänennamen und alternative Domänennamen durch ein Leerzeichen getrennt ein, wie im folgenden Beispiel gezeigt.



4. Das bncert-Tool wird fragen, wie die Umleitung Ihrer Website konfiguriert werden soll. Die folgenden Optionen sind verfügbar:

   - Aktivieren einer Umleitung von HTTP zu HTTPS- Gibt an, ob Benutzer, die zur HTTP-Version Ihrer Website navigieren (d. h.`http:/example.com`) automatisch auf die HTTPS-Version umgeleitet (d.h.`https://example.com`) werden. Wir empfehlen, diese Option zu aktivieren, da sie alle Besucher zwingt, die verschlüsselte Verbindung zu verwenden. `Y` eingeben und Eingabe drücken, um dies zu aktivieren.
   - Umleitung von Nicht-www zu www aktivieren- Gibt an, ob Benutzer, die zur Spitze Ihrer Domäne navigieren (d. h.`https://example.com`) automatisch an die`www`Unterdomäne Ihrer Domäne (d. h.`https://www.example.com`) weitergeleitet werden. Wir empfehlen, diese Option zu auszuwählen. Sie können diese jedoch deaktivieren und die alternative Option aktivieren (aktivieren Sie`www` auf Nicht-`www` Umleiten), wenn Sie die Spitze Ihrer Domäne als bevorzugte Website-Adresse in Suchmaschinentools wie den Webmaster-Tools von Google angegeben haben, oder wenn Ihre Spitze direkt auf Ihre IP verweist und Ihre `www` Unterdomäne Ihren Apex über eine CNAME-Akte referenziert. `Y` eingeben und Eingabe drücken, um dies zu aktivieren.
   - Umleitung von Nicht-www zu www aktivieren- Gibt an, ob Benutzer, die zur Unterdomäne Ihrer Domäne `www` navigieren (d. h.`https://www.example.com`) automatisch an die Spitze Ihrer Domäne (d. h.`https://example.com`) weitergeleitet werden. Wir empfehlen dies zu deaktivieren, wenn Sie Nicht-`www`Umleiten auf`www` aktiviert haben. `N` eingeben und Eingabe drücken, um dies zu aktivieren.

   Ihre Auswahl sollte wie im folgenden Beispiel aussehen.

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.



Enable HTTP to HTTPS redirection [Y/n]: Y



Enable non-www to www redirection [Y/n]: Y



Enable www to non-www redirection [y/N]: N
```

5. Die Änderungen, die vorgenommen werden, sind aufgelistet. Y eingeben undEingabe drücken, um zu bestätigen und fortzufahren.

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
 www.example.com)
7. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

6. Geben Sie Ihre E-Mail-Adresse ein, die Sie Ihrem Let's-Encrypt-Zertifikat zuordnen möchten, und drücken SieEingabe.

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

7. Lesen Sie die Let's-Encrypt-Subscriber-Vereinbarung. Y eingeben undEingabe drücken, um die Vereinbarung zu akzeptieren und fortzufahren.

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

   Die Aktionen werden ausgeführt, um HTTPS für Ihre Instance zu aktivieren, einschließlich der Anforderung des Zertifikats und der Konfiguration der angegebenen Umleitungen.

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.
```

   Ihr Zertifikat wurde erfolgreich ausgestellt und validiert, und die Umleitungen werden erfolgreich für Ihre Instance konfiguriert, wenn eine Meldung ähnlich dem folgenden Beispiel angezeigt wird.

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:
```

   Das `bncert`-Tool führt alle 80 Tage vor Ablauf Ihres Zertifikats eine automatische Erneuerung durch. Fahren Sie mit den nächsten Schritten fort, um die Aktivierung von HTTPS auf Ihrer Website abzuschließen. PrestaShop

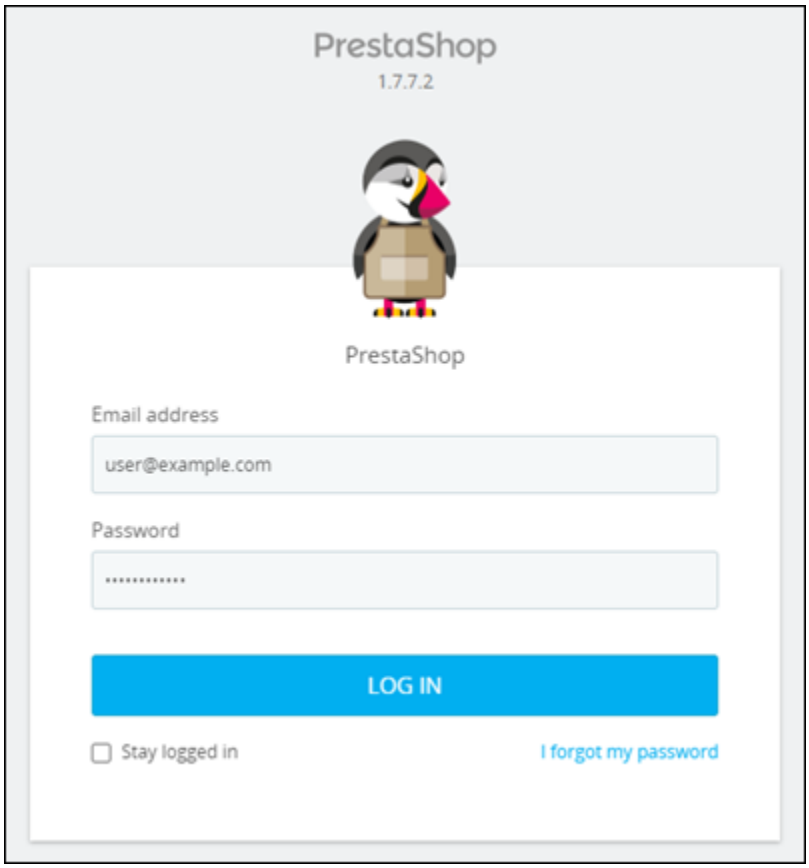
8. Rufen Sie die folgende Adresse auf, um auf die Anmeldeseite für das Administrations-Dashboard Ihrer PrestaShop Website zuzugreifen. Achten Sie darauf, *< DomainName >* durch den registrierten Domainnamen zu ersetzen, der den Traffic zu Ihrer Instance weiterleitet.

```
http://<DomainName>/administration
```

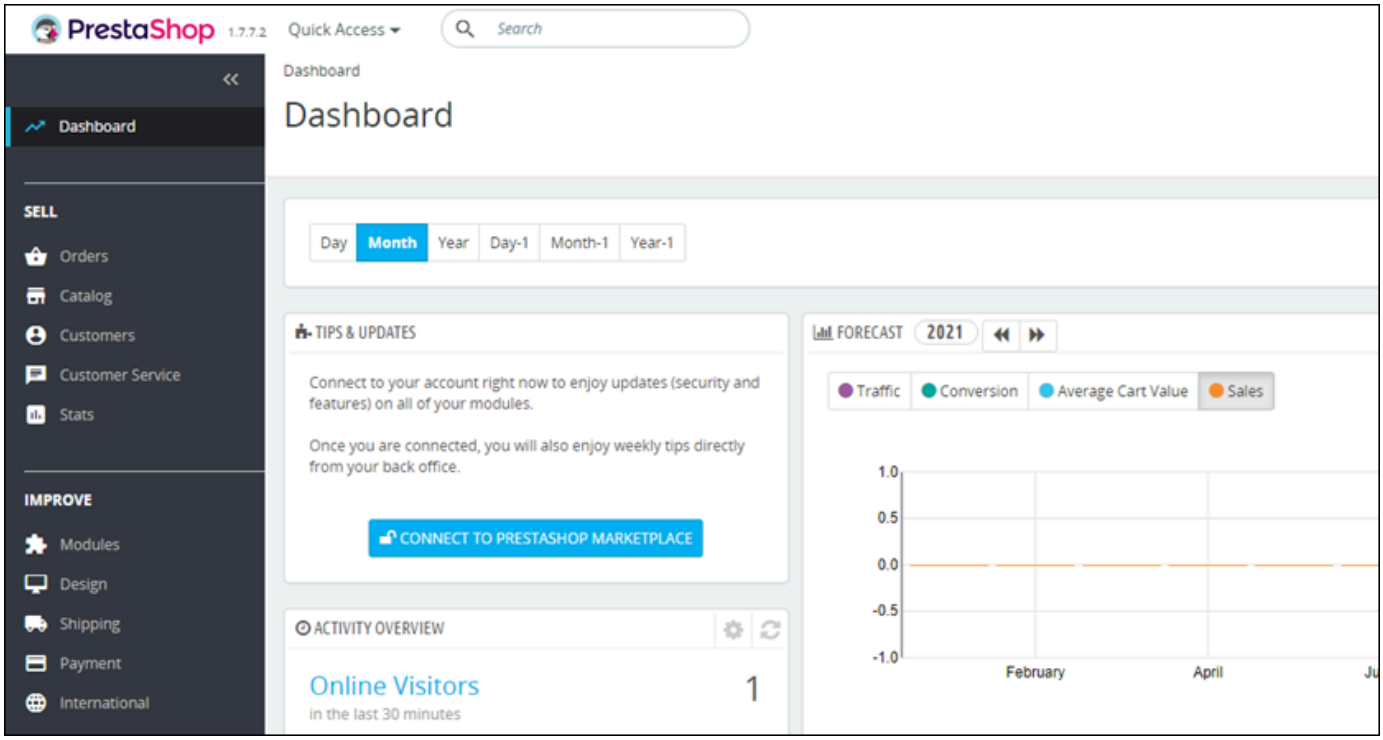
Beispiel:

```
http://www.example.com/administration
```

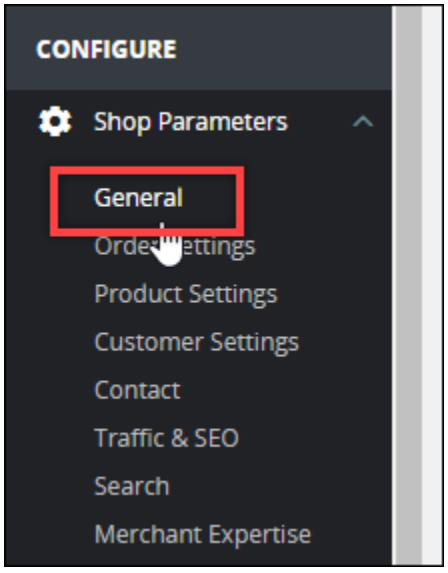
9. Geben Sie den Standard-Benutzernamen ein (`user@example.com`), das Standard-Anwendungspasswort, das Sie zuvor in diesem Leitfaden erhalten haben, und wählen Sie Anmelden aus.



Das PrestaShop Verwaltungs-Dashboard wird angezeigt.



10. Wählen Sie Shop-Parameter im Navigationsbereich und dann Allgemeines.



11. Wählen Sie Ja neben SSL aktivieren aus.

12. Scrollen Sie auf der Seite nach unten und wählen Sie Speichern aus.

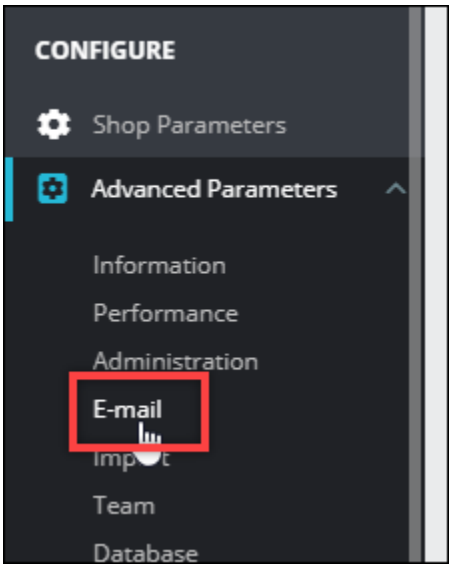
13. Wenn die Seite Allgemeines neu lädt, wählen Sie Ja neben SSL auf allen Seiten aktivieren aus.

14. Scrollen Sie auf der Seite nach unten und wählen Sie Speichern aus.

    HTTPS ist jetzt für Ihre PrestaShop Website konfiguriert. Wenn Kunden die HTTP-Version (z. B.`http://www.example.com`) Ihrer PrestaShop Website aufrufen, werden sie automatisch zur HTTPS-Version (z. B.`https://www.example.com`) weitergeleitet.

Schritt 6: SMTP für E-Mail-Benachrichtigungen konfigurieren

Konfigurieren Sie die SMTP-Einstellungen Ihrer PrestaShop Website, um E-Mail-Benachrichtigungen dafür zu aktivieren. Melden Sie sich dazu im Administrations-Dashboard Ihrer PrestaShop Website an. Wählen Sie Erweiterte Parameter im Navigationsbereich und dann E-mail. Sie sollten Ihre E-Mail-Kontakte auch entsprechend anpassen. Wählen Sie Shop-Parameter im Navigationsbereich und dann Contact (Kontakt).



Weitere Informationen finden Sie PrestaShop im Benutzerhandbuch in der PrestaShop Dokumentation und unter SMTP für ausgehende E-Mails konfigurieren in der Bitnami-Dokumentation.

> **Important**
>
> Wenn Sie SMTP für die Verwendung der Ports 25, 465 oder 587 konfigurieren, müssen Sie diese Ports in der Firewall Ihrer Instanz in der Lightsail-Konsole öffnen. Weitere Informationen finden Sie unter Instance-Firewall-Regeln in Amazon Lightsail hinzufügen und bearbeiten. Wenn Sie Ihr Gmail-Konto für das Senden von E-Mails auf Ihrer PrestaShop Website konfigurieren, müssen Sie ein App-Passwort verwenden, anstatt das Standardpasswort zu verwenden, mit dem Sie sich bei Gmail anmelden. Weitere Informationen finden Sie unter Anmelden mit App-Passwörtern.

Schritt 7: Lesen Sie das Bitnami und die Dokumentation PrestaShop

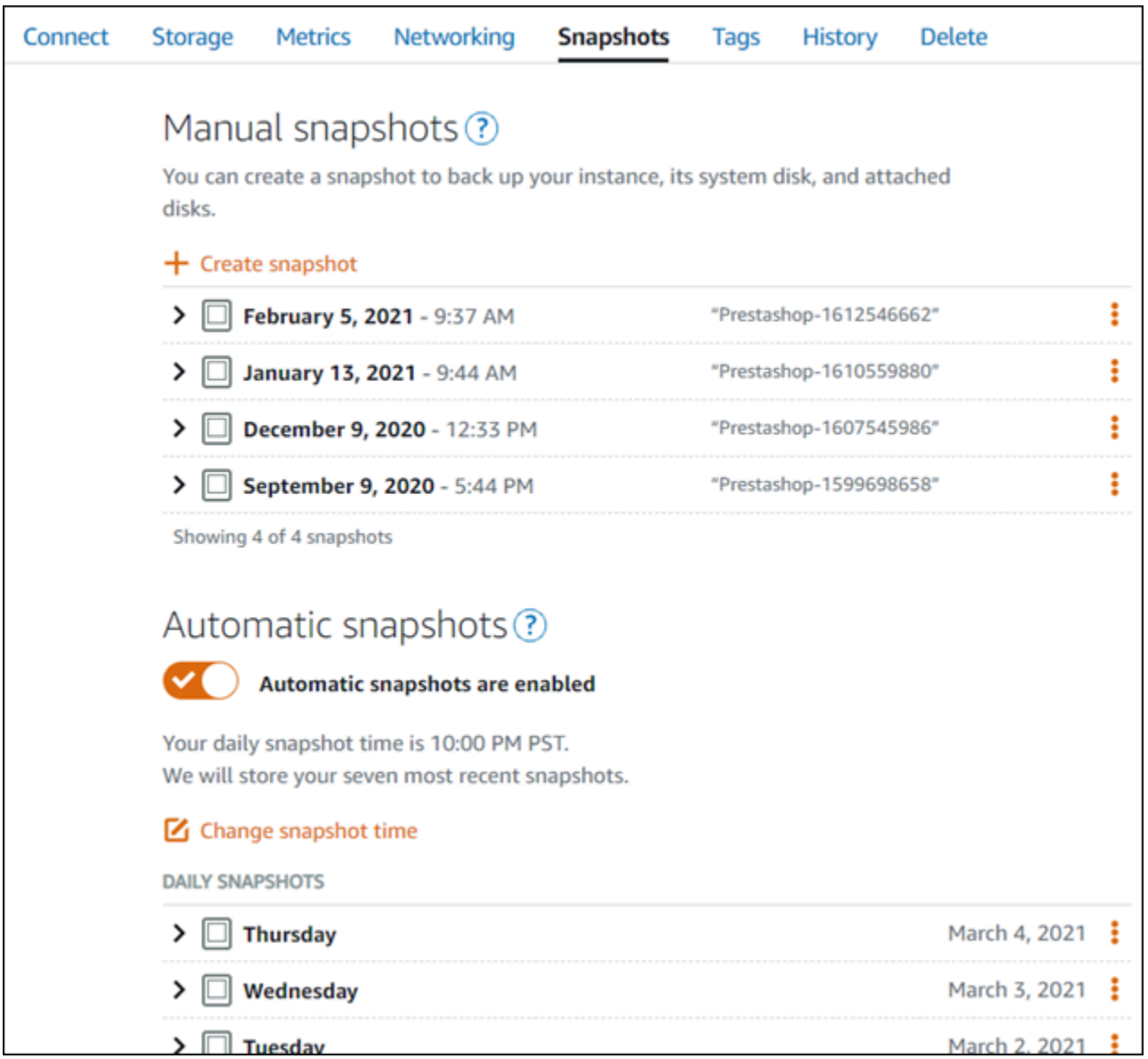
Lesen Sie die Bitnami-Dokumentation, um zu erfahren, wie Sie administrative Aufgaben auf Ihrer PrestaShop Instanz und Website ausführen, z. B. Plugins installieren und das Theme anpassen. Weitere Informationen finden Sie unter Bitnami PrestaShop Stack for AWS Cloud in der Bitnami-Dokumentation.

Sie sollten auch die PrestaShop Dokumentation lesen, um zu erfahren, wie Sie Ihre Website verwalten. PrestaShop Weitere Informationen finden Sie im Benutzerhandbuch PrestaShop in der PrestaShop Dokumentation.

Schritt 8: Erstellen Sie einen Snapshot Ihrer PrestaShop Instance

Nachdem Sie Ihre PrestaShop Website nach Ihren Wünschen konfiguriert haben, erstellen Sie regelmäßig Snapshots Ihrer Instanz, um sie zu sichern. Sie können Schnappschüsse manuell erstellen oder automatische Schnappschüsse aktivieren, damit Lightsail täglich Schnappschüsse für Sie erstellt. Wenn etwas mit Ihrer Instance nicht stimmt, können Sie mit dem Snapshot eine neue Ersatz-Instance erstellen. Weitere Informationen finden Sie unter Snapshots.

Wählen Sie auf der Instance-Verwaltungsseite, unter der RegisterkarteSnapshotSnapshot erstellenoder wählen Sie aus, automatische Snapshots zu aktivieren.



Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Linux- oder Unix-Instance in Amazon Lightsail oder Aktivieren oder Deaktivieren von automatischen Snapshots für Instances oder Festplatten in Amazon Lightsail.

Schnellstartanleitung: Redmine

Hier finden Sie einige erste Schritte, die Sie unternehmen sollten, nachdem Ihre Redmine-Instance auf Amazon Lightsail hochgefahren ist und läuft:

Inhalt

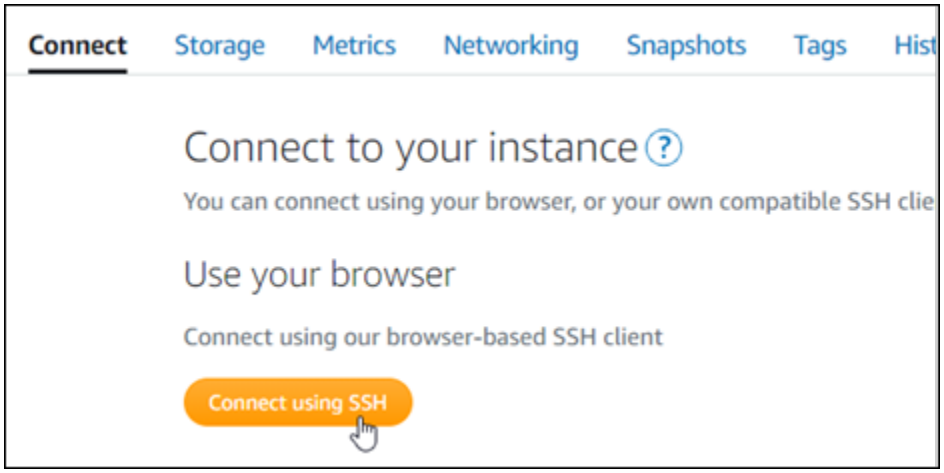
Schritt 1: Die Bitnami-Dokumentation lesen

Lesen Sie die Bitnami-Dokumentation, um zu erfahren, wie Sie Ihre Redmine-Anwendung konfigurieren. Weitere Informationen finden Sie unter Redmine paketiert von Bitnami für AWS Cloud.

Schritt 2: Das Standard-Anwendungspasswort für den Zugriff auf das Redmine-Verwaltungs-Dashboard einholen

Führen Sie das folgende Verfahren durch, um das Standard-Anwendungspasswort für den Zugriff auf das Verwaltungs-Dashboard für Ihre Redmine-Website zu erhalten. Weitere Informationen finden Sie unter Abrufen des Anwendungs-Benutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.

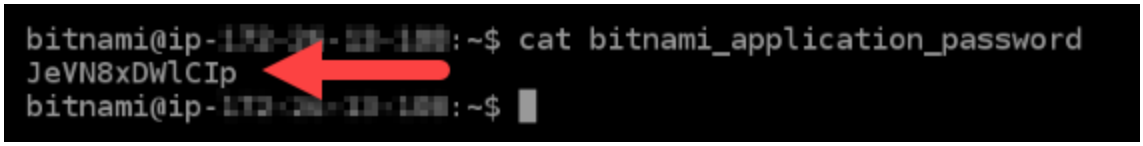
1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um das Anwendungspasswort zu erhalten:

```
cat $HOME/bitnami_application_password
```

Sie sollten eine ähnliche Antwort wie diese sehen, die das Standard-Anwendungspasswort enthält:



Schritt 3: Ihrer Instance eine statische IP-Adresse anfügen

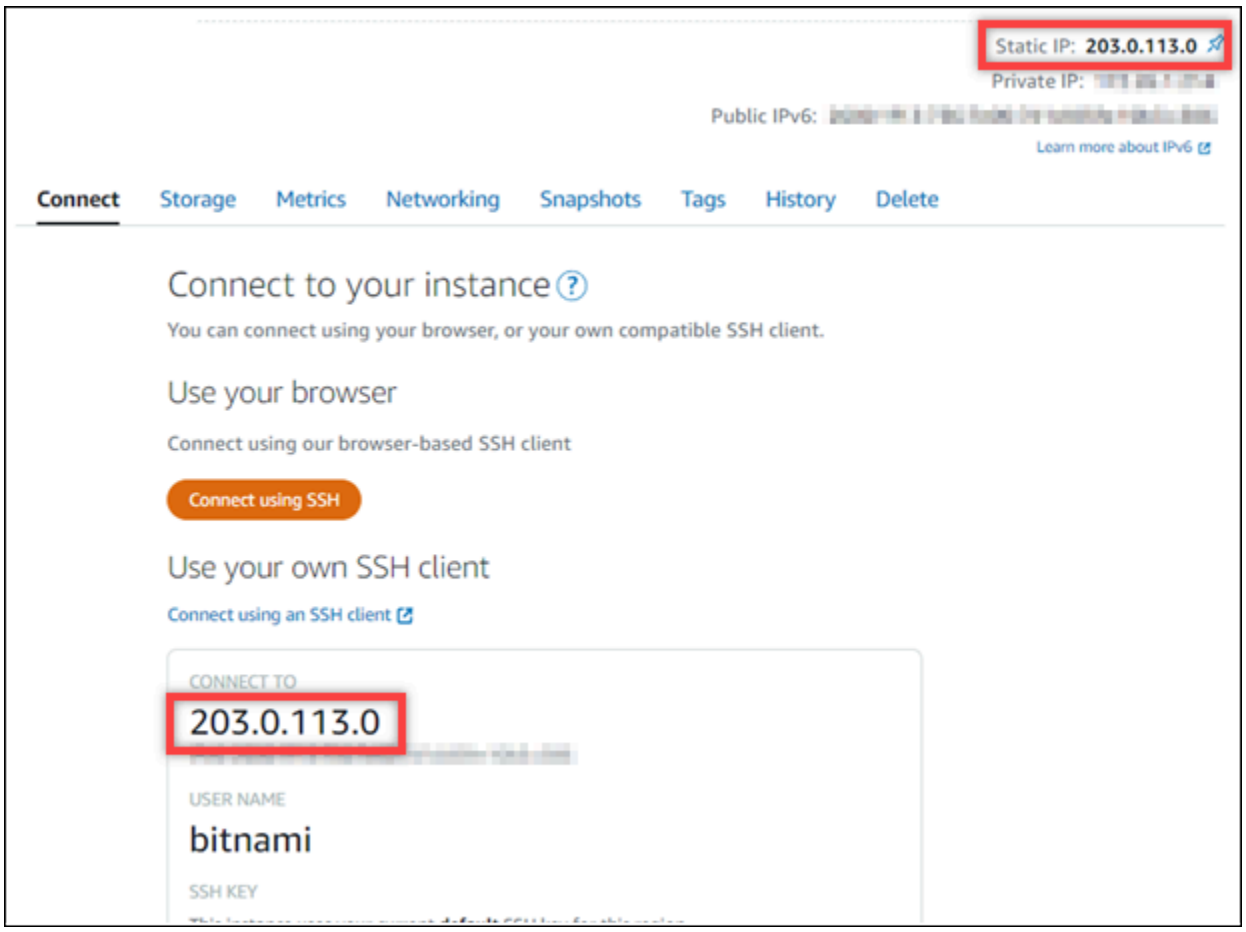
Die Ihrer Instance beim ersten Erstellen zugewiesene öffentliche IP-Adresse ändert sich bei jedem Stopp und Start Ihrer Instance. Sie sollten eine statische IP-Adresse erstellen und an Ihre Instance anfügen, um sicherzustellen, dass sich deren öffentliche IP-Adresse nicht ändert. Wenn Sie Ihrer Instance später einen registrierten Domänennamen wie zum Beispiel `example.com` zuweisen, müssen Sie nicht jedes Mal, wenn Sie Ihre Instance stoppen und neu starten, die DNS-Akte Ihrer Domäne aktualisieren. Sie können eine statische IP an eine Instance anhängen.

Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Netzwerk, die Registerkarte Erstellen einer statischen IP oder Anfügen einer statischen IP (falls Sie zuvor eine statische IP-Adresse erstellt haben, die Sie Ihrer Instance anfügen können) und folgen Sie dann den Anweisungen auf der Seite. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

Schritt 4: Beim Verwaltungs-Dashboard für Ihre Redmine-Website anmelden

Nachdem Sie nun das Standard-Anwendungspasswort haben, führen Sie das folgende Verfahren aus, um zur Homepage Ihrer Redmine-Website zu navigieren und sich beim Verwaltungs-Dashboard anzumelden. Nachdem Sie angemeldet sind, können Sie Ihre Website anpassen und administrative Änderungen vornehmen. Weitere Informationen zu den Möglichkeiten in Joomla! finden Sie im Abschnitt Schritt 7: Die Redmine-Dokumentation lesen und Ihre Website weiter konfigurieren weiter unten in diesem Leitfaden.

1. Notieren Sie sich von Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die öffentliche IP-Adresse Ihrer Instance. Die öffentliche IP-Adresse wird auch im Kopfzeilenabschnitt Ihrer Instance-Verwaltungsseite angezeigt.



2. Navigieren Sie zur öffentlichen IP-Adresse ihrer Instance, indem Sie z B. zu `http://203.0.113.0` gehen.

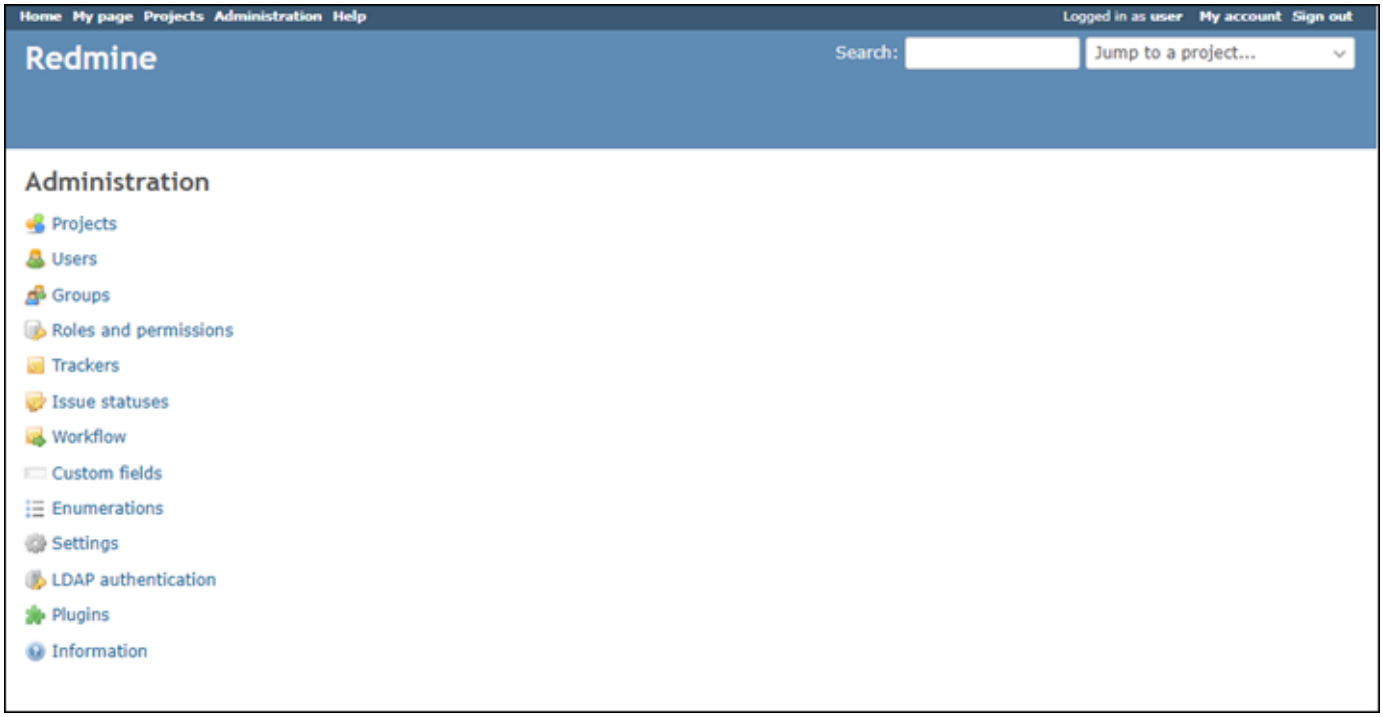
   Die Startseite Ihrer Redmine-Website sollte erscheinen.

3. Wählen Sie Manage (Verwalten) in der unteren rechten Ecke Ihrer Startseite der Redmine-Website.

   Wenn das Banner Manage (Verwalten) nicht angezeigt wird, können Sie die Anmeldeseite erreichen, indem Sie zu `http://<PublicIP>/admin` gehen. Ersetzen Sie *<PublicIP>* durch die öffentliche IP-Adresse Ihrer Instance.

4. Melden Sie sich mit dem Standardbenutzernamen (`user`) und dem zuvor abgerufenen Standardpasswort an, wie vorhin in diesem Leitfaden beschrieben.

   Das Redmine-Verwaltungs-Dashboard wird angezeigt.



Schritt 5: Datenverkehr für Ihren registrierten Domänennamen auf Ihre Redmine-Website weiterleiten

Um den Datenverkehr für Ihren registrierten Domänennamen, z. B. `example.com`, auf Ihrer Redmine-Website weiterzuleiten, fügen Sie zum DNS Ihrer Domäne eine Akte hinzu. DNS-Datensätze werden in der Regel beim Registrar verwaltet und gehostet, bei dem Sie Ihre Domäne registriert haben. Wir empfehlen jedoch, die Verwaltung der DNS-Datensätze Ihrer Domäne auf Lightsail zu übertragen, damit Sie sie über die Lightsail-Konsole verwalten können.

Wählen Sie auf der Startseite der Lightsail-Konsole unter der Registerkarte Domains & DNS (Domains und DNS) die Option Create DNS zone (DNS-Zone erstellen) und folgen Sie dann den Anweisungen auf der Seite. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain in Lightsail.

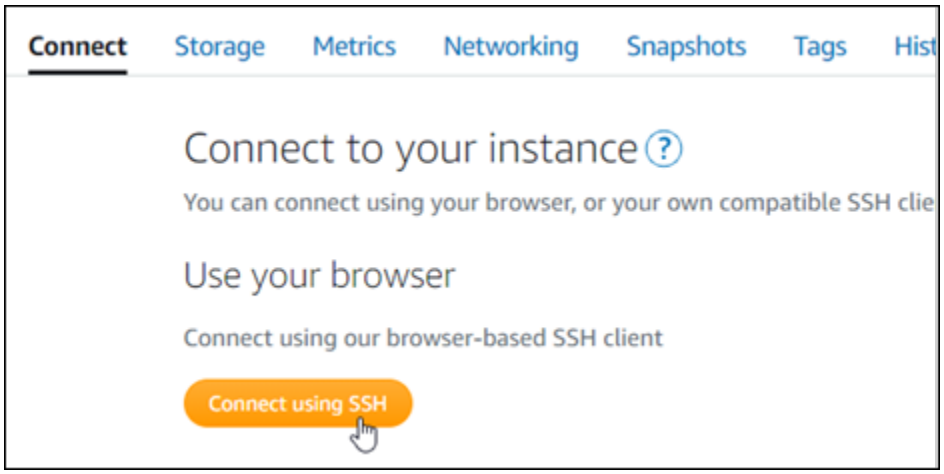
Wenn Sie zu dem Domänennamen navigieren, den Sie für Ihre Instance konfiguriert haben, sollten Sie zur Startseite Ihrer Redmine-Website umgeleitet werden. Als Nächstes sollten Sie ein SSL/TLS-Zertifikat erstellen und konfigurieren, um HTTPS-Verbindungen für Ihre Redmine-Website zu ermöglichen. Für weitere Informationen fahren Sie mit dem nächsten Abschnitt Schritt 6: HTTPS für Ihre Redmine-Website konfigurieren in diesem Leitfaden fort.

Schritt 6: HTTPS für Ihre Redmine-Website konfigurieren

Führen Sie die folgenden Schritte aus, um HTTPS auf Ihrer Redmine-Website zu konfigurieren. Diese Schritte zeigen Ihnen, wie Sie das Bitnami-HTTPS-Konfigurations-Tool (`bncert-tool`) verwenden, ein Befehlszeilentool zum Anfordern von SSL/TLS-Zertifikaten von Let's Encrypt. Weitere Informationen finden Sie unter Erfahren Sie mehr über das Bitnami-HTTPS-Konfigurations-Tool in der Bitnami-Dokumentation.

> **Important**
>
> Bevor Sie mit diesem Verfahren beginnen, stellen Sie sicher, dass Sie Ihre Domäne so konfiguriert haben, dass der Datenverkehr an Ihre Redmine-Instance weitergeleitet wird. Andernfalls schlägt die SSL/TLS-Zertifikatvalidierung fehl.

1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um zu bestätigen, dass das bncert-Tool auf Ihrer Instance installiert ist.

```
sudo /opt/bitnami/bncert-tool
```

   Sie sollten eine der folgenden Antworten sehen:

   - Wenn Sie den Befehl in der Antwort nicht gefunden haben, ist das bncert-Tool auf Ihrer Instance nicht installiert. Fahren Sie mit dem nächsten Schritt in diesem Verfahren fort, um das bncert-Tool auf Ihrer Instance zu installieren.

- Wenn in der Antwort Willkommen beim HTTPS-Konfigurationstool von Bitnami angezeigt wird, ist das bncert-Tool auf Ihrer Instance installiert. Fahren Sie mit Schritt 8 dieses Verfahrens fort.
- Wenn das bncert-Tool bereits eine Zeit lang auf Ihrer Instance installiert ist, wird möglicherweise eine Meldung angezeigt, die angibt, dass eine aktualisierte Version des Tools verfügbar ist. Wählen Sie, es herunterzuladen, und geben Sie dann den `sudo /opt/bitnami/bncert-tool`-Befehl ein, um das bncert-Tool erneut auszuführen. Fahren Sie mit Schritt 8 dieses Verfahrens fort.

3. Geben Sie den folgenden Befehl ein, um die bncert-Laufdatei auf Ihre Instance herunterzuladen.

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. Geben Sie den folgenden Befehl ein, um ein Verzeichnis für die bncert-Tool-Laufdatei auf Ihrer Instance zu erstellen.

```
sudo mkdir /opt/bitnami/bncert
```

5. Geben Sie den folgenden Befehl ein, um die bncrt-Laufdatei als ein Programm auszuführen.

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. Geben Sie den folgenden Befehl ein, um einen symbolischen Link zu erstellen, der das bncert-Tool ausführt, wenn Sie den Befehl sudo /opt/bitnami/bncert-tool eingeben.

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

Sie sind jetzt fertig mit der Installation des bncert-Tools auf Ihrer Instance.

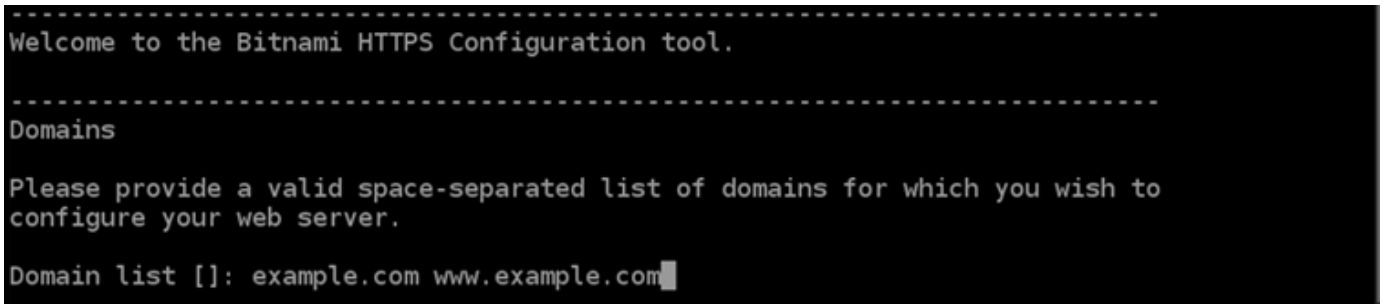
7. Geben Sie den folgenden Befehl ein, um das bncert-Tool auszuführen.

```
sudo /opt/bitnami/bncert-tool
```

8. Geben Sie Ihren primären Domänennamen und alternative Domänennamen durch ein Leerzeichen getrennt ein, wie im folgenden Beispiel gezeigt.

Wenn Ihre Domäne nicht darauf konfiguriert ist, Datenverkehr auf die öffentliche IP-Adresse Ihrer Instance umzuleitent, wird das`bncert`-Tool Sie aufgefordern, diese Konfiguration vorzunehmen, bevor Sie fortfahren. Ihre Domäne muss den Datenverkehr an die öffentliche IP-Adresse der Instance weiterleiten, von der Sie das `bncert`-Tool verwenden, um HTTPS für die Instance zu

aktivieren. Dies bestätigt, dass Sie Eigentümer der Domäne sind und dient als Validierung für Ihr Zertifikat.



9. Das `bncert`-Tool wird Sie fragen, wie die Umleitung Ihrer Website konfiguriert werden soll. Die folgenden Optionen sind verfügbar:

   - Aktivieren einer Umleitung von HTTP zu HTTPS- Gibt an, ob Benutzer, die zur HTTP-Version Ihrer Website navigieren (d. h.`http:/example.com`) automatisch auf die HTTPS-Version umgeleitet (d.h.`https://example.com`) werden. Wir empfehlen, diese Option zu aktivieren, da sie alle Besucher zwingt, die verschlüsselte Verbindung zu verwenden. `Y` eingeben und Eingabe drücken, um dies zu aktivieren.
   - Umleitung von Nicht-www zu www aktivieren- Gibt an, ob Benutzer, die zur Spitze Ihrer Domäne navigieren (d. h.`https://example.com`) automatisch an die`www`Unterdomäne Ihrer Domäne (d. h.`https://www.example.com`) weitergeleitet werden. Wir empfehlen, diese Option zu auszuwählen. Sie können diese jedoch deaktivieren und die alternative Option aktivieren (aktivieren Sie`www` auf Nicht-`www` Umleiten), wenn Sie die Spitze Ihrer Domäne als bevorzugte Website-Adresse in Suchmaschinentools wie den Webmaster-Tools von Google angegeben haben, oder wenn Ihre Spitze direkt auf Ihre IP verweist und Ihre `www` Unterdomäne Ihren Apex über eine CNAME-Akte referenziert. `Y` eingeben und Eingabe drücken, um dies zu aktivieren.
   - Umleitung von Nicht-www zu www aktivieren- Gibt an, ob Benutzer, die zur Unterdomäne Ihrer Domäne `www` navigieren (d. h.`https://www.example.com`) automatisch an die Spitze Ihrer Domäne (d. h.`https://example.com`) weitergeleitet werden. Wir empfehlen dies zu deaktivieren, wenn Sie Nicht-`www`Umleiten auf`www` aktiviert haben. `N` eingeben und Eingabe drücken, um dies zu aktivieren.

   Ihre Auswahl sollte wie im folgenden Beispiel aussehen.

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.



Enable HTTP to HTTPS redirection [Y/n]: Y



Enable non-www to www redirection [Y/n]: Y



Enable www to non-www redirection [y/N]: N
```

10. Die Änderungen, die vorgenommen werden, sind aufgelistet. Y eingeben undEingabe drücken, um zu bestätigen und fortzufahren.

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
 www.example.com)
7. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

11. Geben Sie Ihre E-Mail-Adresse ein, die Sie Ihrem Let's-Encrypt-Zertifikat zuordnen möchten, und drücken SieEingabe.

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

12. Lesen Sie die Let's-Encrypt-Subscriber-Vereinbarung. Y eingeben undEingabe drücken, um die Vereinbarung zu akzeptieren und fortzufahren.

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

Die Aktionen werden ausgeführt, um HTTPS für Ihre Instance zu aktivieren, einschließlich der Anforderung des Zertifikats und der Konfiguration der angegebenen Umleitungen.

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.
```

Ihr Zertifikat wurde erfolgreich ausgestellt und validiert, und die Umleitungen werden erfolgreich für Ihre Instance konfiguriert, wenn eine Meldung ähnlich dem folgenden Beispiel angezeigt wird.

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:
```

Das `bncert`-Tool führt alle 80 Tage vor Ablauf Ihres Zertifikats eine automatische Erneuerung durch. Wiederholen Sie die obigen Schritte, wenn Sie zusätzliche Domänen und Unterdomänen mit Ihrer Instance verwenden möchten und Sie HTTPS für diese Domänen aktivieren möchten.

Sie sind jetzt fertig, HTTPS auf Ihrer Redmine-Instance zu aktivieren. Wenn Sie das nächste Mal mit der von Ihnen konfigurierten Domäne zu Ihrer Redmine-Website navigieren, sollten Sie sehen, dass sie auf die HTTPS-Verbindung umgeleitet wird.

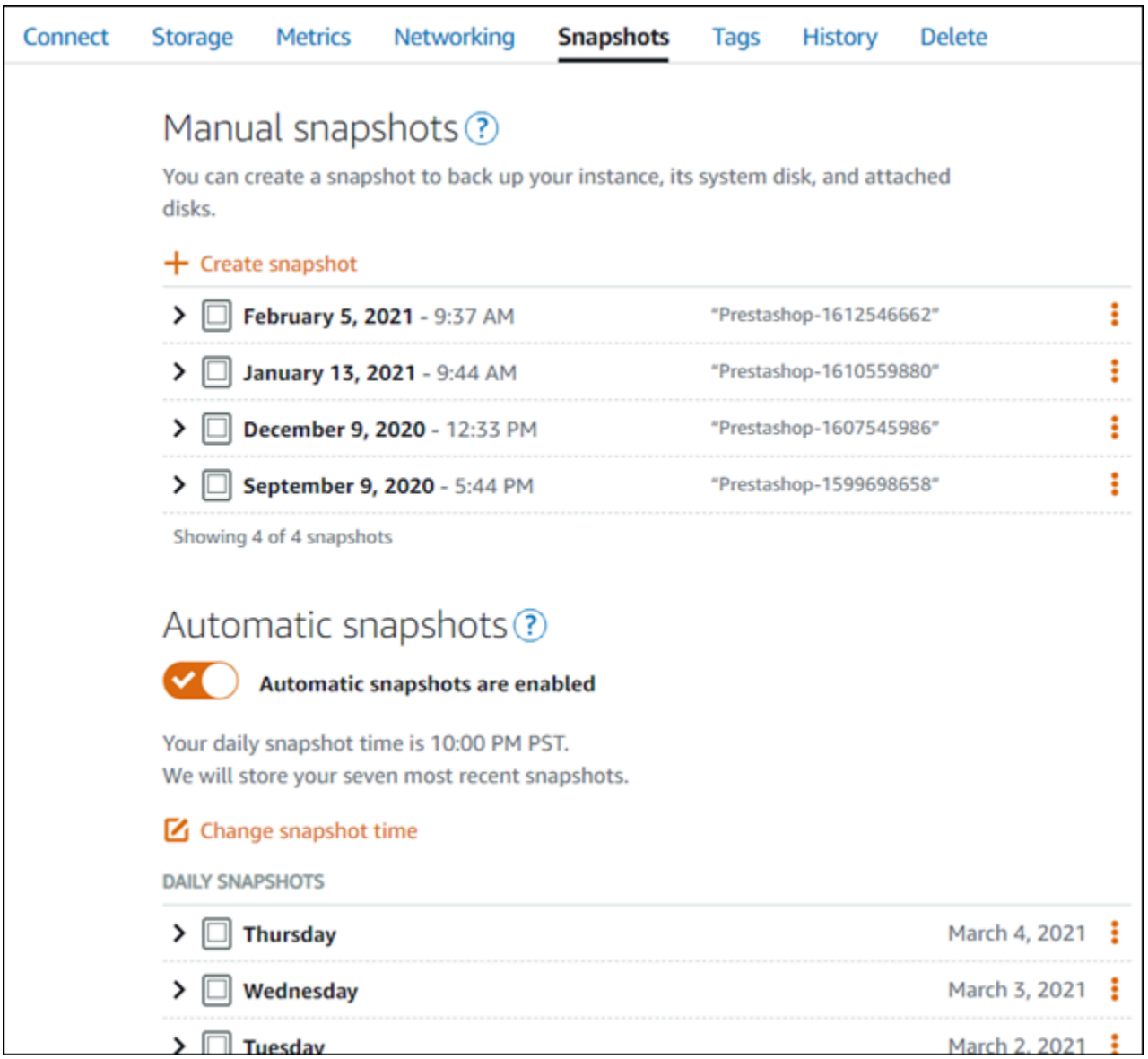
Schritt 7: Die Redmine-Dokumentation lesen und Ihre Website weiter konfigurieren

Lesen Sie die Redmine-Dokumentation, um zu erfahren, wie Sie Ihre Website verwalten und anpassen. Weitere Informationen finden Sie im Redmine-Benutzerhandbuch.

Schritt 8: Einen Snapshot Ihrer Instance erstellen

Nachdem Sie Ihre Redmine-Website so konfiguriert haben, wie Sie sie möchten, erstellen Sie periodische Snapshots Ihrer Instance, um diese zu sichern. Sie können Snapshots manuell erstellen oder automatische Snapshots aktivieren, damit Lightsail tägliche Snapshots für Sie erstellt.. Wenn etwas mit Ihrer Instance nicht stimmt, können Sie mit dem Snapshot eine neue Ersatz-Instance erstellen. Weitere Informationen finden Sie unter Snapshots.

Wählen Sie auf der Instance-Verwaltungsseite, unter der RegisterkarteSnapshotSnapshot erstellenoder wählen Sie aus, automatische Snapshots zu aktivieren.



Weitere Informationen finden Sie unter Erstellen eines Snapshots IhrerLinux- oder Unix-Instance inAmazon LightsailoderAktivieren oder Deaktivieren von automatischen Snapshots für Instances oder Datenträger inAmazon Lightsail.

Schnellstartanleitung: WordPress

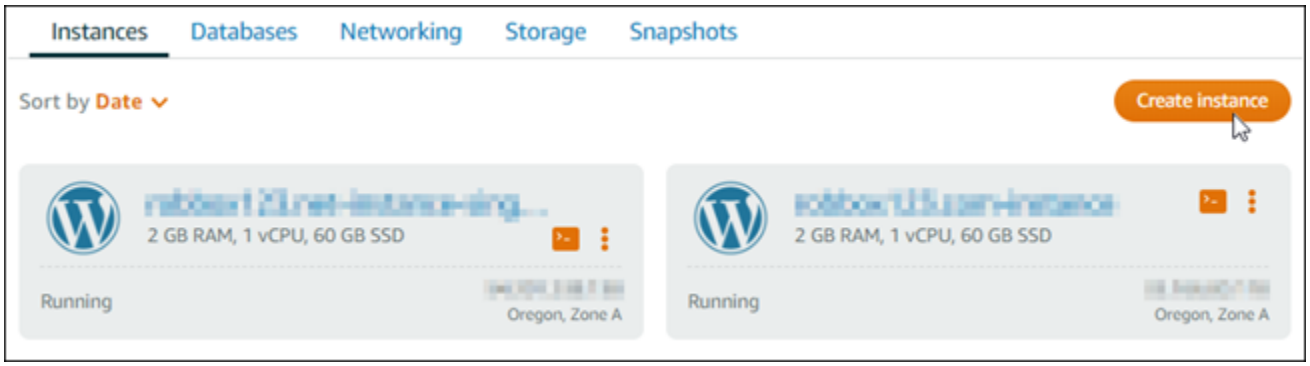
In dieser Schnellstartanleitung erfahren Sie, wie Sie eine WordPress Instance auf Amazon Lightsail starten und konfigurieren.

Schritt 1: Eine Instance erstellen WordPress

Führen Sie die folgenden Schritte aus, um Ihre WordPress Instance zum Laufen zu bringen.

So erstellen Sie eine Lightsail-Instanz für WordPress

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite im Abschnitt Instances die Option Create instance aus.



3. Wählen Sie die Availability Zone AWS-Region und die Availability Zone für Ihre Instance aus.

4. Wählen Sie das Image für Ihre Instanz wie folgt aus:
   a. Wählen Sie unter Plattform auswählen die Option Linux/Unix.
   b. Wählen Sie für Wählen Sie einen Blueprint aus. WordPress
5. Wählen Sie einen Instance-Plan.

Ein Plan beinhaltet eine Maschinenkonfiguration (RAM, SSD, vCPU) zu niedrigen, vorhersehbaren Kosten sowie eine Datenübertragungsgebühr.

6. Geben Sie einen Namen für Ihre Instance ein. Ressourcennamen:

   - Muss AWS-Region in Ihrem Lightsail-Konto jeweils einzigartig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

7. Wählen Sie Create instance (Instance erstellen).
8. Um den Test-Blogbeitrag anzusehen, rufen Sie die Instanzverwaltungsseite auf und kopieren Sie die öffentliche IPv4-Adresse, die in der oberen rechten Ecke der Seite angezeigt wird. Fügen Sie die Adresse in das Adressfeld eines mit dem Internet verbundenen Webbrowsers ein. Der Browser zeigt den Test-Blogbeitrag an.

Schritt 2: Konfigurieren Sie Ihre WordPress Instanz

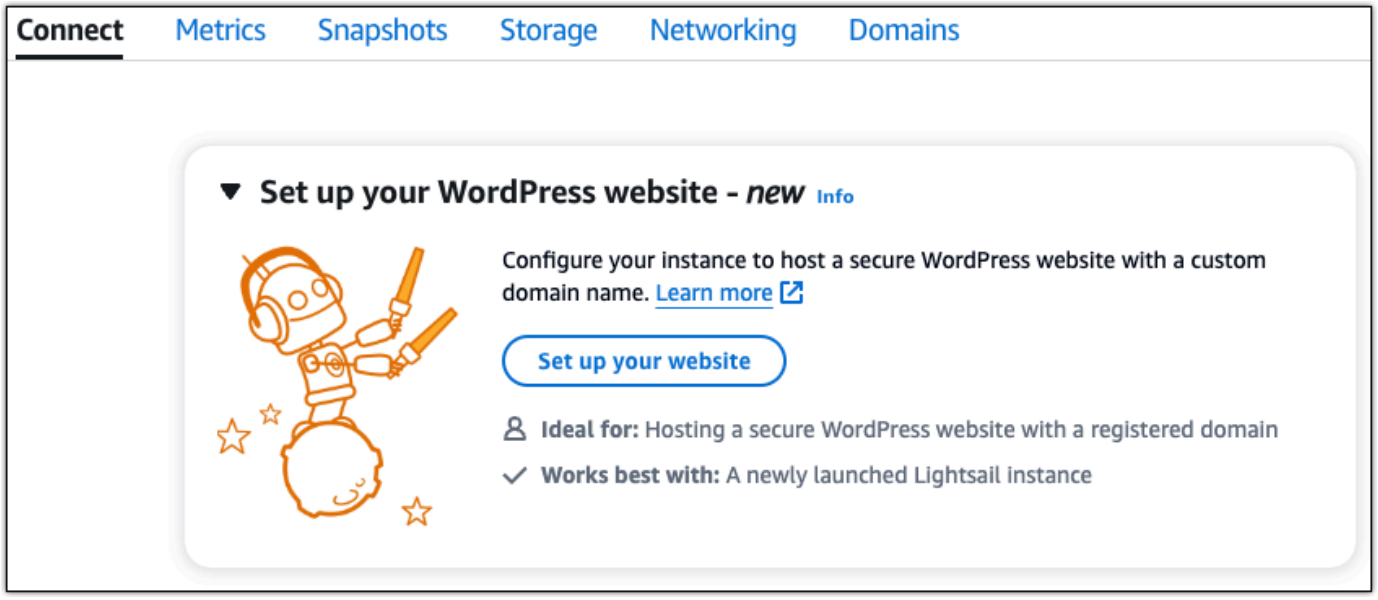
Sie können Ihre WordPress Instanz mithilfe eines geführten step-by-step Workflows konfigurieren, der Folgendes konfiguriert:

- Ein registrierter Domainname — Ihre WordPress Website benötigt einen Domainnamen, den Sie sich leicht merken können. Benutzer geben diesen Domainnamen an, um auf Ihre WordPress Site zuzugreifen. Weitere Informationen finden Sie unter Domains und DNS.
- DNS-Verwaltung — Sie müssen entscheiden, wie Sie die DNS-Einträge für Ihre Domain verwalten möchten. Ein DNS-Eintrag teilt dem DNS-Server mit, welcher IP-Adresse oder welchem Hostnamen eine Domain oder Subdomain zugeordnet ist. Eine DNS-Zone enthält die DNS-Einträge für Ihre Domain. Weitere Informationen finden Sie unter the section called “DNS in Lightsail”.
- Eine statische IP-Adresse — Die öffentliche Standard-IP-Adresse für Ihre WordPress Instance ändert sich, wenn Sie Ihre Instance beenden und starten. Wenn Sie Ihrer Instance eine statische IP-Adresse zuordnen, bleibt sie auch dann unverändert, wenn Sie Ihre Instance beenden und starten. Weitere Informationen finden Sie unter the section called “IP-Adressen”.
- Ein SSL/TLS-Zertifikat — Nachdem Sie ein validiertes Zertifikat erstellt und es auf Ihrer Instance installiert haben, können Sie HTTPS für Ihre WordPress Website aktivieren, sodass der Datenverkehr, der über Ihre registrierte Domain an die Instance weitergeleitet wird, mit HTTPS verschlüsselt wird. Weitere Informationen finden Sie unter the section called “HTTPS aktivieren”.

> **Tip**
>
> Lesen Sie sich die folgenden Tipps durch, bevor Sie beginnen. Informationen zur Problembehandlung finden Sie unter Problembehandlung bei der WordPress Einrichtung.
>
> - Setup unterstützt Lightsail-Instanzen mit WordPress Version 6 und neuer, die nach dem 1. Januar 2023 erstellt wurden.
> - Ihre Instanz muss sich im Status Running befinden. Warten Sie einige Minuten, bis die SSH-Verbindung bereit ist, falls die Instanz gerade gestartet wurde.
> - Die Ports 22, 80 und 443 auf Ihrer Instanz-Firewall müssen TCP-Verbindungen von jeder IP-Adresse aus zulassen, während das Setup läuft. Weitere Informationen finden Sie unter Instance-Firewalls.
> - Wenn Sie DNS-Einträge hinzufügen oder aktualisieren, die auf Traffic von Ihrer Apex-Domain (`example.com`) und deren `www` Subdomänen (`www.example.com`) verweisen, müssen sie sich über das Internet verbreiten. Sie können überprüfen, ob Ihre DNS-Änderungen wirksam wurden, indem Sie Tools wie nslookup oder DNS Lookup from verwenden. MxToolbox
> - WordPress-Instanzen, die vor dem 1. Januar 2023 erstellt wurden, enthalten möglicherweise ein veraltetes Certbot Personal Package Archive (PPA) -Repository, das dazu führt, dass die Einrichtung der Website fehlschlägt. Wenn dieses Repository während der Einrichtung vorhanden ist, wird es aus dem vorhandenen Pfad entfernt und an dem folgenden Speicherort auf Ihrer Instanz gesichert:. `~/opt/bitnami/lightsail/repo.backup` Weitere Informationen zum veralteten PPA finden Sie unter Certbot PPA auf der Canonical-Website.
> - Let's Encrypt-Zertifikate werden automatisch alle 60 bis 90 Tage erneuert.
> - Stoppen Sie Ihre Instanz nicht und nehmen Sie während des Setups keine Änderungen daran vor. Die Konfiguration Ihrer Instance kann bis zu 15 Minuten dauern. Sie können den Fortschritt für jeden Schritt auf der Registerkarte Instanzverbindung einsehen.

So konfigurieren Sie Ihre Instanz mit dem Website-Einrichtungsassistenten

1. Wählen Sie auf der Instanzverwaltungsseite auf dem Tab Connect die Option Website einrichten aus.



2. Verwenden Sie für Specify a domain name eine bestehende von Lightsail verwaltete Domain, registrieren Sie eine neue Domain bei Lightsail oder verwenden Sie eine Domain, die Sie über einen anderen Domain-Registrar registriert haben. Wählen Sie Diese Domain verwenden, um mit dem nächsten Schritt fortzufahren.
3. Führen Sie für Configure DNS einen der folgenden Schritte aus:
   - Wählen Sie von Lightsail verwaltete Domain, um eine Lightsail-DNS-Zone zu verwenden. Wählen Sie Diese DNS-Zone verwenden, um mit dem nächsten Schritt fortzufahren.
   - Wählen Sie Drittanbieter-Domain, um den Hosting-Dienst zu nutzen, der die DNS-Einträge für Ihre Domain verwaltet. Beachten Sie, dass wir eine passende DNS-Zone in Ihrem Lightsail-Konto erstellen, falls Sie diese später verwenden möchten. Wählen Sie DNS eines Drittanbieters verwenden, um mit dem nächsten Schritt fortzufahren.
4. Geben Sie unter Statische IP-Adresse erstellen einen Namen für Ihre statische IP-Adresse ein und wählen Sie dann Statische IP-Adresse erstellen aus.
5. Wählen Sie für Domainzuweisungen verwalten die Option Zuweisung hinzufügen, wählen Sie einen Domain-Typ und dann Hinzufügen aus. Wählen Sie Weiter, um mit dem nächsten Schritt fortzufahren.
6. Wählen Sie für Create an SSL/TLS certificate Ihre Domains und Subdomains aus, geben Sie eine E-Mail-Adresse ein, wählen Sie Ich autorisiere Lightsail, ein Let's Encrypt-Zertifikat auf meiner Instanz zu konfigurieren, und wählen Sie Zertifikat erstellen aus. Wir beginnen mit der Konfiguration der Lightsail-Ressourcen.

Stoppen Sie Ihre Instanz nicht und nehmen Sie während des Setups keine Änderungen daran vor. Die Konfiguration Ihrer Instance kann bis zu 15 Minuten dauern. Sie können den Fortschritt für jeden Schritt auf der Registerkarte Instanzverbindung einsehen.

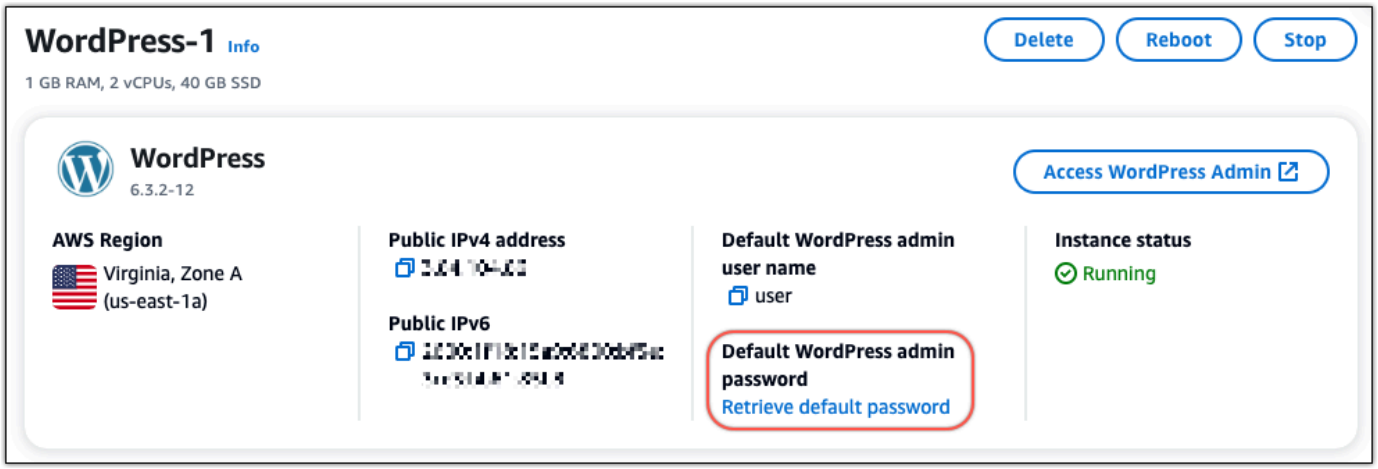
7. Nachdem die Einrichtung der Website abgeschlossen ist, vergewissern Sie sich, dass die URLs, die Sie im Schritt Domainzuweisungen angegeben haben, Ihre WordPress Website öffnen.

Schritt 3: Holen Sie sich das Standardanwendungskennwort für Ihre WordPress Website

Sie benötigen das Standardanwendungskennwort, um sich im Administrations-Dashboard für Ihre WordPress Website anzumelden.

Um das Standardkennwort für den WordPress Administrator zu erhalten

1. Öffnen Sie die Instanzverwaltungsseite für Ihre WordPress Instanz.
2. Wählen Sie im WordPressPanel die Option Standardkennwort abrufen aus. Dadurch wird das Access-Standardkennwort unten auf der Seite erweitert.



3. Wählen Sie Launch. CloudShell Dadurch wird unten auf der Seite ein Fenster geöffnet.
4. Wählen Sie Kopieren und fügen Sie den Inhalt dann in das CloudShell Fenster ein. Sie können entweder den Cursor auf die CloudShell Eingabeaufforderung setzen und Strg+V drücken, oder Sie können mit der rechten Maustaste klicken, um das Menü zu öffnen, und dann Einfügen wählen.
5. Notieren Sie sich das im CloudShell Fenster angezeigte Passwort. Sie benötigen es, um sich im Administrations-Dashboard Ihrer WordPress Website anzumelden.

```
[cloudshell-user@ip-[redacted] ~]$ AWS_REGION=us-east-1 ~/lightsail_connect WordPress-1 cat bitnami_applic
ation_password
JKzh8wB5FAR!
```

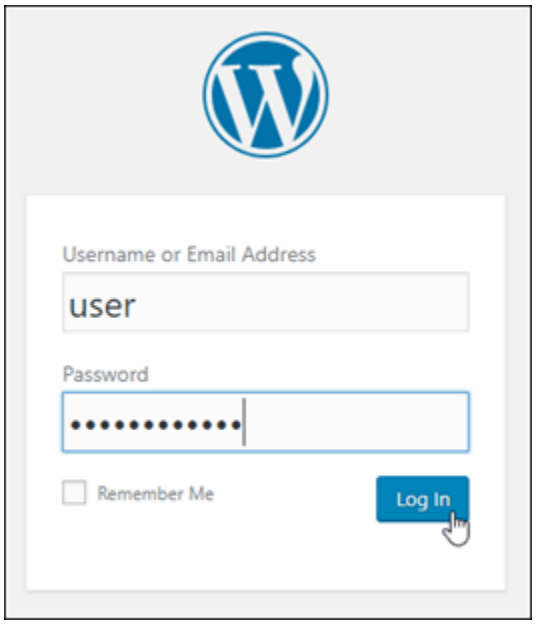
Schritt 4: Melden Sie sich auf Ihrer Website an WordPress

Nachdem Sie das Standardbenutzerpasswort haben, navigieren Sie zur Startseite Ihrer WordPress Website und melden Sie sich im Administrations-Dashboard an. Nachdem Sie angemeldet sind, können Sie das Standardpasswort ändern.

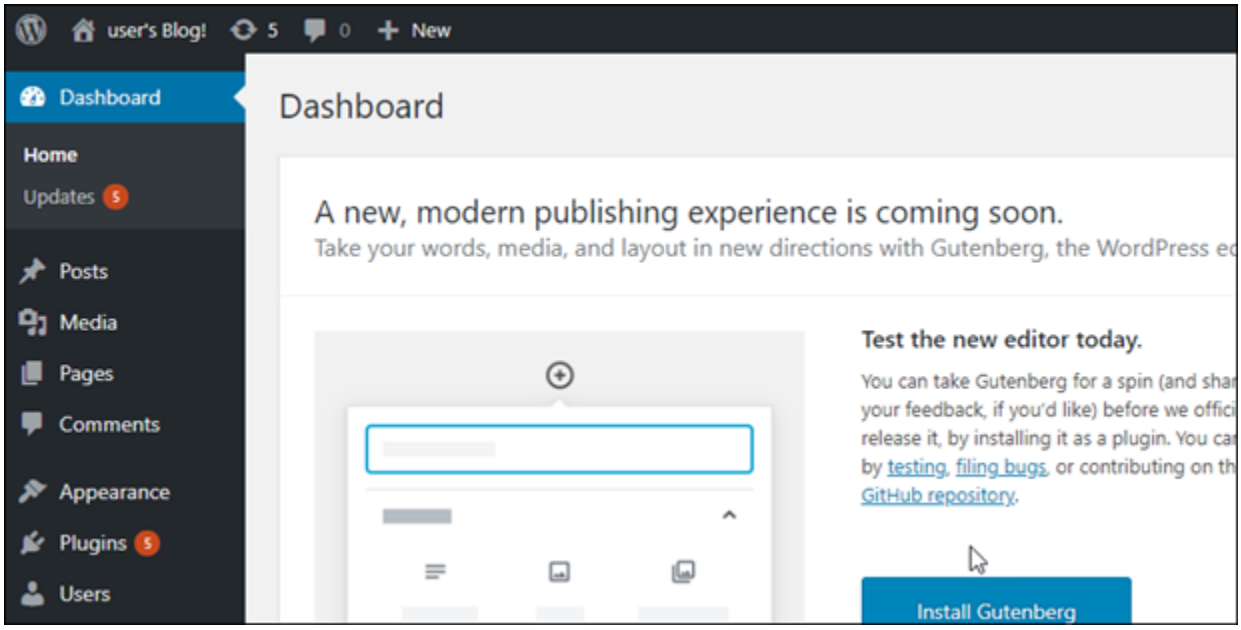
Um sich im Administrations-Dashboard anzumelden

1. Öffnen Sie die Instanzverwaltungsseite für Ihre WordPress Instanz.
2. Wählen Sie im WordPressPanel Access WordPress Admin aus.
3. Wählen Sie im Bereich Access your WordPress Admin Dashboard unter Öffentliche IP-Adresse verwenden den Link mit dem folgenden Format aus:

   http://*public-ipv4-Adresse*. /wp-admin
4. Geben Sie als Benutzername oder E-Mail-Adresse ein. **`user`**
5. Geben Sie unter Passwort das Passwort ein, das Sie im vorherigen Schritt erhalten haben.
6. Wählen Sie Log in (Anmelden).



Sie sind jetzt im Administrations-Dashboard Ihrer WordPress Website angemeldet, wo Sie administrative Aktionen ausführen können. Weitere Informationen zur Verwaltung Ihrer WordPress Website finden Sie im WordPressCodex in der WordPress Dokumentation.



Schritt 5: Lesen Sie die Bitnami-Dokumentation

Lesen Sie die Bitnami-Dokumentation, um zu erfahren, wie Sie administrative Aufgaben auf Ihrer WordPress Website ausführen, z. B. Plugins installieren, das Theme anpassen und Ihre Version von aktualisieren. WordPress

Weitere Informationen finden Sie in der WordPress Bitnami-Dokumentation für. AWS Cloud

Schnellstartanleitung: WordPress Multisite

Hier finden Sie einige erste Schritte, die Sie unternehmen sollten, nachdem Ihre WordPress-Multisite-Instance auf Amazon Lightsail hochgefahren ist und läuft:

Inhalt

- Schritt 5: Den Datenverkehr für Ihren registrierten Domänennamen auf Ihre WordPress-Multisite-Website weiterleiten
- Schritt 6: Blogs als Domänen oder Subdomänen zu Ihrer WordPress-Multisite-Website hinzufügen
- Schritt 7: Die WordPress-Multisite-Dokumentation lesen und Ihre Website weiter konfigurieren
- Schritt 8: Einen Snapshot Ihrer Instance erstellen

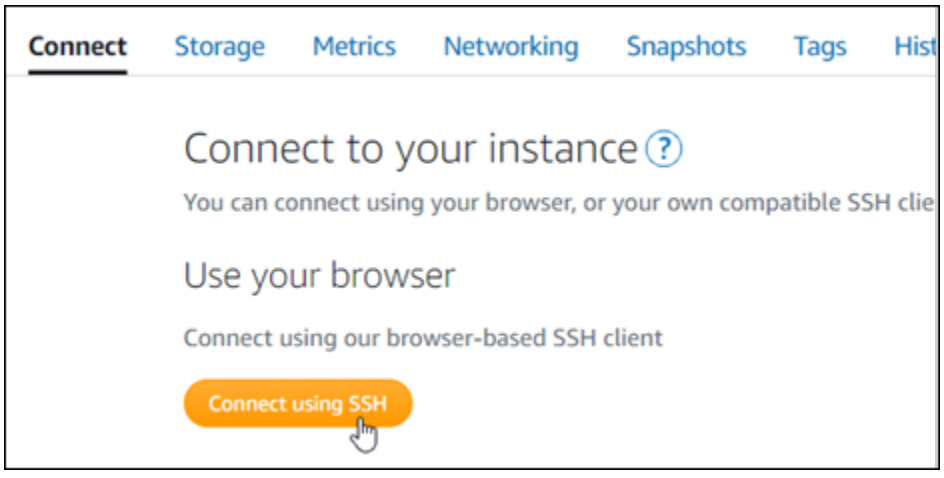
Schritt 1: Die Bitnami-Dokumentation lesen

Lesen Sie die Bitnami-Dokumentation, um zu erfahren, wie Sie Ihre WordPress-Multisite-Instance konfigurieren. Weitere Informationen finden Sie unter WordPress Multisite paketiert von Bitnami für AWS Cloud.

Schritt 2: Das Standard-Anwendungspasswort für den Zugriff auf das WordPress-Verwaltungs-Dashboard einholen

Führen Sie das folgende Verfahren aus, um das Standard-Anwendungspasswort zu erhalten, das für den Zugriff auf das Verwaltungs-Dashboard Ihrer WordPress-Multisite-Website erforderlich ist. Weitere Informationen finden Sie unter Abrufen des Anwendungs-Benutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.

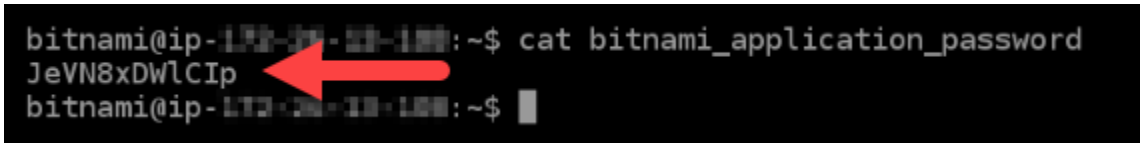
1. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein, um das Standard-Anwendungspasswort zu erhalten:

```
cat $HOME/bitnami_application_password
```

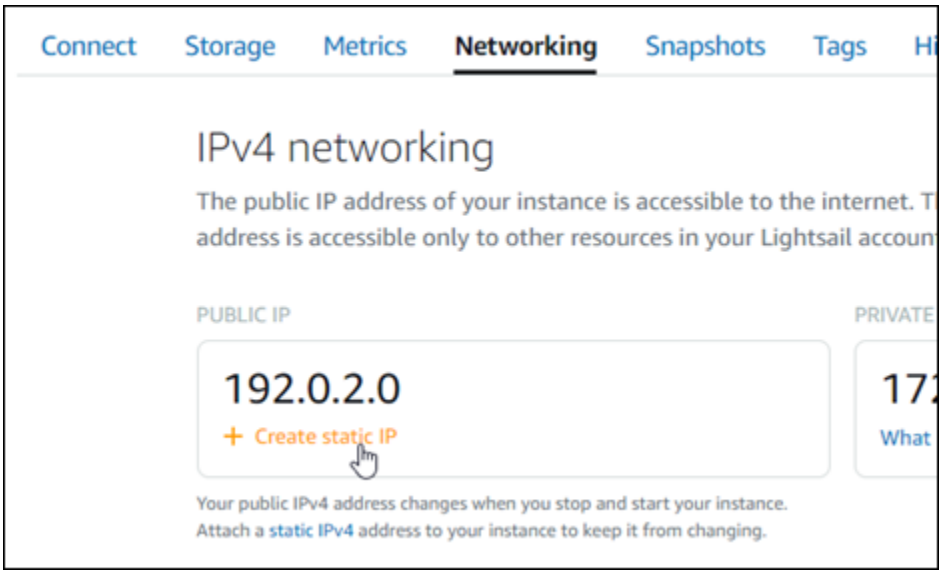
Sie sollten eine ähnliche Antwort wie diese sehen, die das Standard-Anwendungspasswort enthält. Verwenden Sie dieses Passwort, um sich beim Verwaltungs-Dashboard Ihrer WordPress-Multisite-Website anzumelden.



Schritt 3: Ihrer Instance eine statische IP-Adresse anfügen

Die Ihrer Instance beim ersten Erstellen zugewiesene öffentliche IP-Adresse ändert sich bei jedem Stopp und Start Ihrer Instance. Sie sollten eine statische IP-Adresse erstellen und an Ihre Instance anfügen, um sicherzustellen, dass sich deren öffentliche IP-Adresse nicht ändert. Wenn Sie später Ihren registrierten Domänennamen wie zum Beispiel `example.com`, mit Ihrer Instance verwenden, müssen Sie nicht jedes Mal, wenn Sie Ihre Instance stoppen und neu starten, das Domain Name System (DNS) Ihrer Domäne aktualisieren. Sie können eine statische IP an eine Instance anhängen.

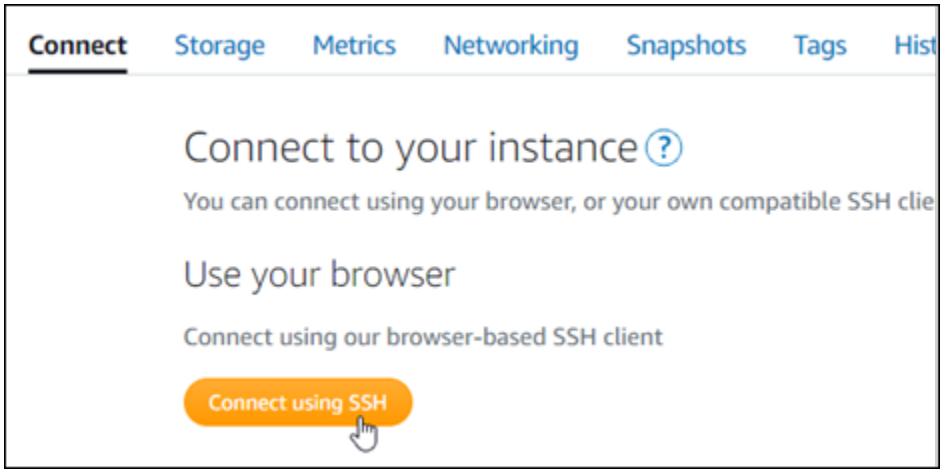
Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Netzwerk, die Registerkarte Erstellen einer statischen IP oder Anfügen einer statischen IP (falls Sie zuvor eine statische IP-Adresse erstellt haben, die Sie Ihrer Instance anfügen können) und folgen Sie dann den Anweisungen auf der Seite. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.



Nachdem die neue statische IP-Adresse an Ihre Instance angefügt wurde, müssen Sie die folgenden Schritte ausführen, um WordPress auf die neue statische IP-Adresse aufmerksam zu machen.

1. Notieren Sie sich die neue statische IP-Adresse Ihrer Instance. Sie wird im Kopfzeilenabschnitt Ihrer Instance-Verwaltungsseite aufgeführt.

2. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Verbinden die Option Verbinden mit SSH.



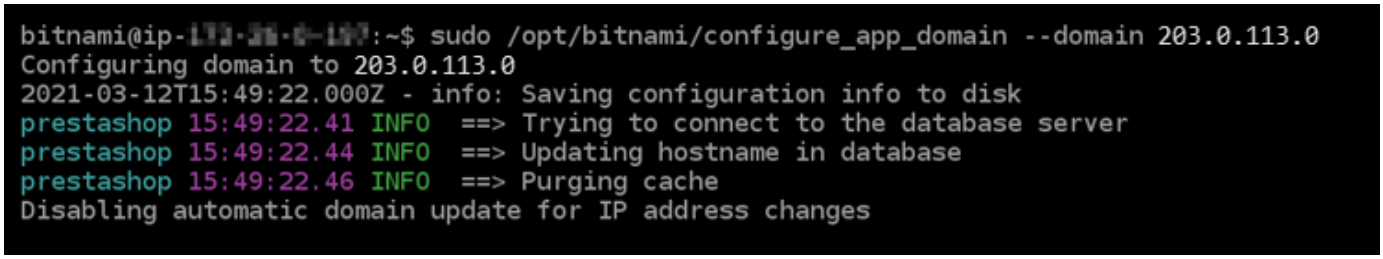
3. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein. Stellen Sie sicher, dass Sie *<StaticIP>* mit der neuen statischen IP-Adresse Ihrer Instance ersetzen.

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

Beispiel:

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

Sie sollten eine Reaktion ähnlich dem folgenden Beispiel erhalten. Die WordPress-Website auf Ihrer Instance sollte nun die neue statische IP-Adresse erkannt haben.



Wenn dieser Befehl fehlschlägt, verwenden Sie möglicherweise eine ältere Version der WordPress-Multisite-Instance. Versuchen Sie, stattdessen die folgenden Befehle auszuführen. Stellen Sie sicher, dass Sie *<StaticIP>* mit der neuen statischen IP-Adresse Ihrer Instance ersetzen.

```
cd /opt/bitnami/apps/wordpress
sudo ./bnconfig --machine_hostname <StaticIP>
```

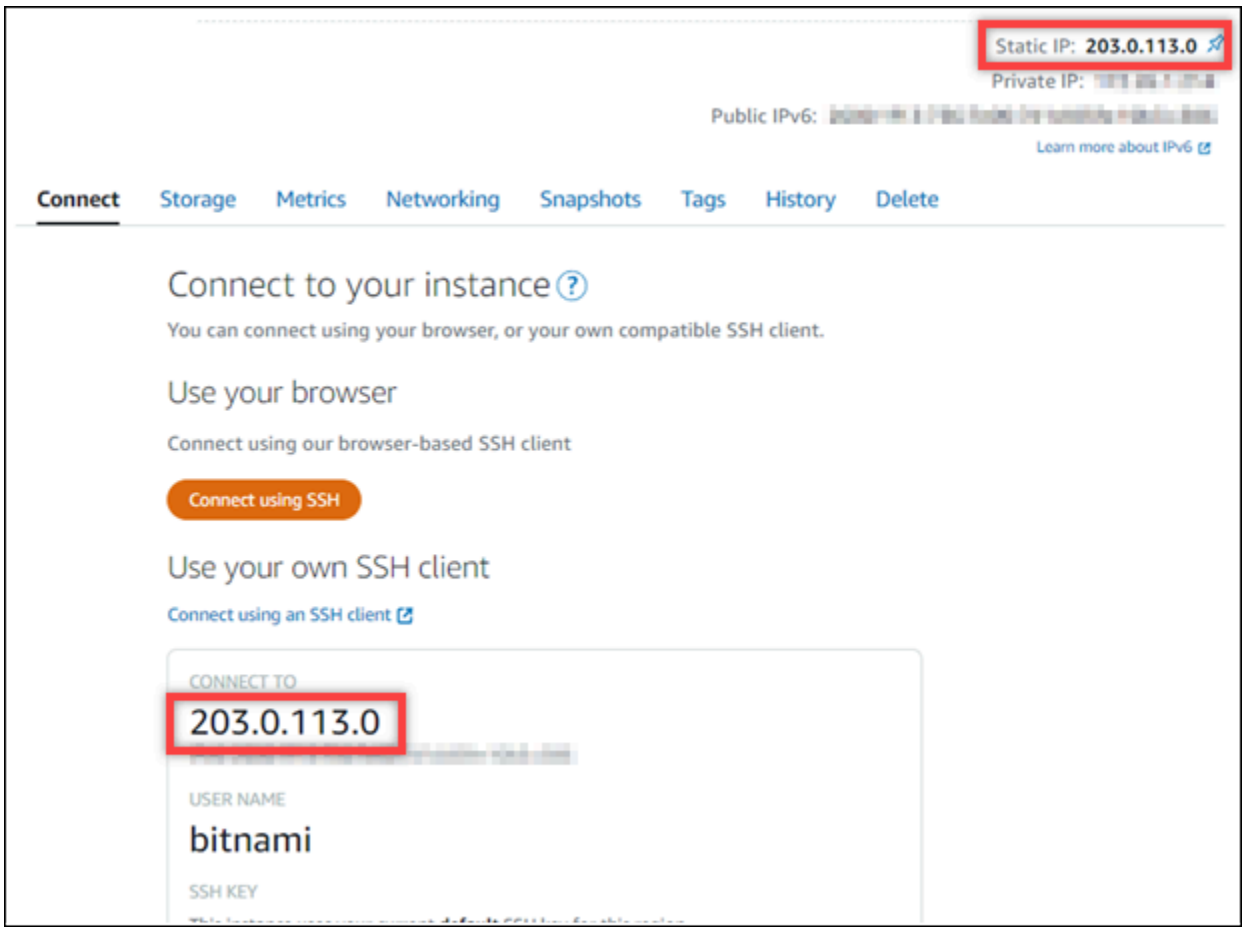
Nachdem diese Befehle ausgeführt wurden, geben Sie den folgenden Befehl ein, um zu verhindern, dass das bnconfig-Tool bei jedem Neustart des Servers automatisch ausgeführt wird.

```
sudo mv bnconfig bnconfig.disabled
```

Schritt 4: Beim Verwaltungs-Dashboard für Ihre WordPress-Multisite-Website anmelden

Nachdem Sie nun das Standard-Benutzerpasswort haben, navigieren Sie zur Startseite Ihrer WordPress-Multisite-Website und melden Sie sich im Verwaltungs-Dashboard an. Nachdem Sie angemeldet sind, können Sie Ihre Website anpassen und administrative Änderungen vornehmen. Weitere Informationen zu den Möglichkeiten in WordPress finden Sie im Abschnitt Schritt 7: Die WordPress-Multisite-Dokumentation lesen und Ihre Website weiter konfigurieren weiter unten in diesem Leitfaden.

1. Notieren Sie sich von Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die öffentliche IP-Adresse Ihrer Instance. Die öffentliche IP-Adresse wird auch im Kopfzeilenabschnitt Ihrer Instance-Verwaltungsseite angezeigt.



2. Navigieren Sie zur öffentlichen IP-Adresse ihrer Instance, indem Sie z B. zu `http://203.0.113.0` gehen.

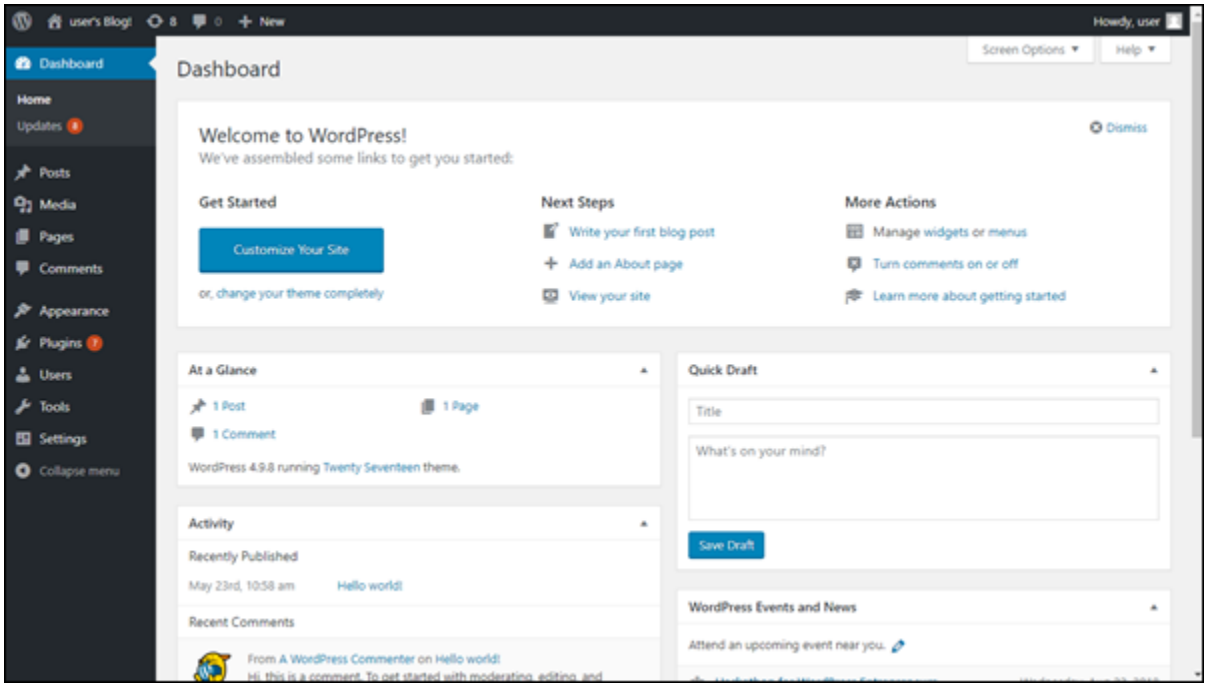
   Die Startseite Ihrer WordPress-Website sollte erscheinen.

3. Wählen Sie Manage (Verwalten) in der unteren rechten Ecke Ihrer Startseite der WordPress-Website.

   Wenn das Banner Manage (Verwalten) nicht angezeigt wird, können Sie die Anmeldeseite erreichen, indem Sie zu `http://<PublicIP>/wp-login.php` gehen. Ersetzen Sie *`<PublicIP>`* durch die öffentliche IP-Adresse Ihrer Instance.

4. Melden Sie sich mit dem Standardbenutzernamen (`user`) und dem zuvor abgerufenen Standardpasswort an, wie vorhin in diesem Leitfaden beschrieben.

   Das WordPress Administrations-Dashboard wird angezeigt.



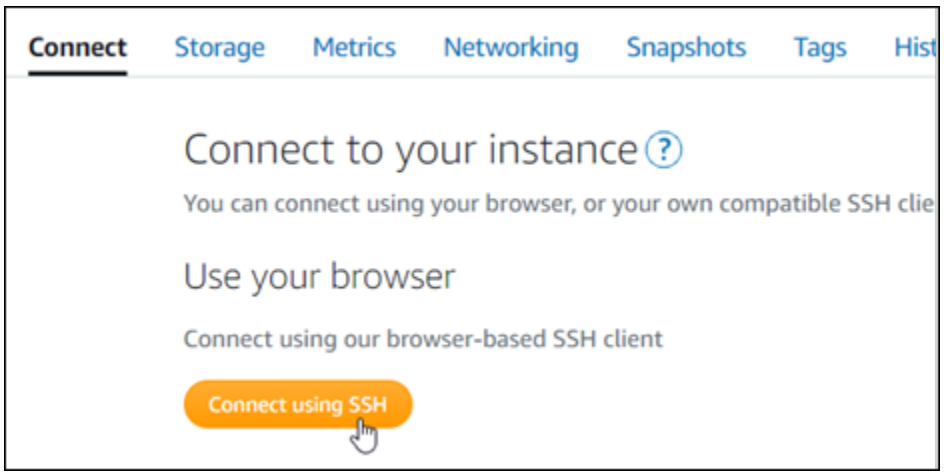
Schritt 5: Den Datenverkehr für Ihren registrierten Domänennamen auf Ihre WordPress-Multisite-Website weiterleiten

Um den Datenverkehr für Ihren registrierten Domänennamen, wie z. B. `example.com` auf Ihrer WordPress-Multisite-Website weiterzuleiten, fügen Sie zum DNS Ihrer Domäne eine Akte hinzu. DNS-Datensätze werden in der Regel beim Registrar verwaltet und gehostet, bei dem Sie Ihre Domäne registriert haben. Wir empfehlen jedoch, die Verwaltung der DNS-Datensätze Ihrer Domäne auf Lightsail zu übertragen, damit Sie sie über die Lightsail-Konsole verwalten können.

Wählen Sie auf der Startseite der Lightsail-Konsole unter der Registerkarte Domains & DNS (Domains und DNS) die Option Create DNS zone (DNS-Zone erstellen) und folgen Sie dann den Anweisungen auf der Seite. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain in Lightsail.

Nachdem Ihr Domänenname Datenverkehr an Ihre Instance weitergeleitet hat, müssen Sie die folgenden Schritte ausführen, um die WordPress auf den Domänennamen aufmerksam zu machen.

1. Wählen Sie auf der Instance-Verwaltungsseite unter der Registerkarte Verbinden die Option Verbinden mit SSH.



2. Nachdem Sie verbunden sind, geben Sie den folgenden Befehl ein. Ersetzen Sie *<DomainName>* mit dem Domänennamen, der den Datenverkehr an Ihre Instance weiterleitet.

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

Beispiel:

```
sudo /opt/bitnami/configure_app_domain --domain www.example.com
```

Sie sollten eine Reaktion ähnlich dem folgenden Beispiel erhalten. Die WordPress-Multisite-Software sollte nun den Domänennamen erkannt haben.

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain www.example.com
Configuring domain to www.example.com
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

Wenn dieser Befehl fehlschlägt, verwenden Sie möglicherweise eine ältere Version der WordPress-Multisite-Instance. Versuchen Sie, stattdessen die folgenden Befehle auszuführen. Ersetzen Sie *<DomainName>* mit dem Domänennamen, der den Datenverkehr an Ihre Instance weiterleitet.

```
cd /opt/bitnami/apps/wordpress
sudo ./bnconfig --machine_hostname <DomainName>
```

Nachdem diese Befehle ausgeführt wurden, geben Sie den folgenden Befehl ein, um zu verhindern, dass das bnconfig-Tool bei jedem Neustart des Servers automatisch ausgeführt wird.

```
sudo mv bnconfig bnconfig.disabled
```

Wenn Sie zu dem Domänennamen navigieren, den Sie für Ihre Instance konfiguriert haben, sollten Sie zum Hauptblog Ihrer WordPress-Multisite-Website weitergeleitet werden. Als nächstes müssen Sie entscheiden, ob Sie Blogs als Domänen oder als Subdomänen zu Ihrer WordPress-Multisite-Website hinzufügen möchten. Für weitere Informationen fahren Sie mit dem nächsten Abschnitt Schritt 6: Blogs als Domänen oder Subdomänen zu Ihrer WordPress-Multisite-Website hinzufügen in diesem Leitfaden fort.

Schritt 6: Blogs als Domänen oder Subdomänen zu Ihrer WordPress-Multisite-Website hinzufügen

WordPress Multisite wurde entwickelt, um mehrere Blog-Websites auf einer Instance von WordPress zu hosten. Wenn Sie Ihrer WordPress-Multisite neue Blog-Websites hinzufügen, können Sie sie so konfigurieren, dass sie ihre eigenen Domänen oder eine Subdomäne der primären Domäne Ihrer WordPress-Multisite verwenden. Sie können Ihre WordPress-Multisite so konfigurieren, dass sie nur eine dieser Optionen verwendet. Wenn Sie beispielsweise Blog-Sites als Domänen hinzufügen möchten, können Sie keine Blog-Sites als Subdomänen hinzufügen und umgekehrt. Informationen zum Konfigurieren dieser Optionen finden Sie jeweils in einer der folgenden Anleitungen:

- Informationen zum Hinzufügen von Blogseiten als Domänen wie `example1.com` und `example2.com` finden Sie unter Hinzufügen von Blogs als Domänen zu Ihrer WordPress-Multisite-Instance in Lightsail.
- Um Blog-Sites als Subdomänen der primären Domain Ihrer WordPress-Multisite hinzuzufügen, wie z. B. `one.example.com` und `two.example.com`, siehe Hinzufügen von Blogs als Subdomänen zu Ihrer WordPress-Multisite-Instance in Lightsail.

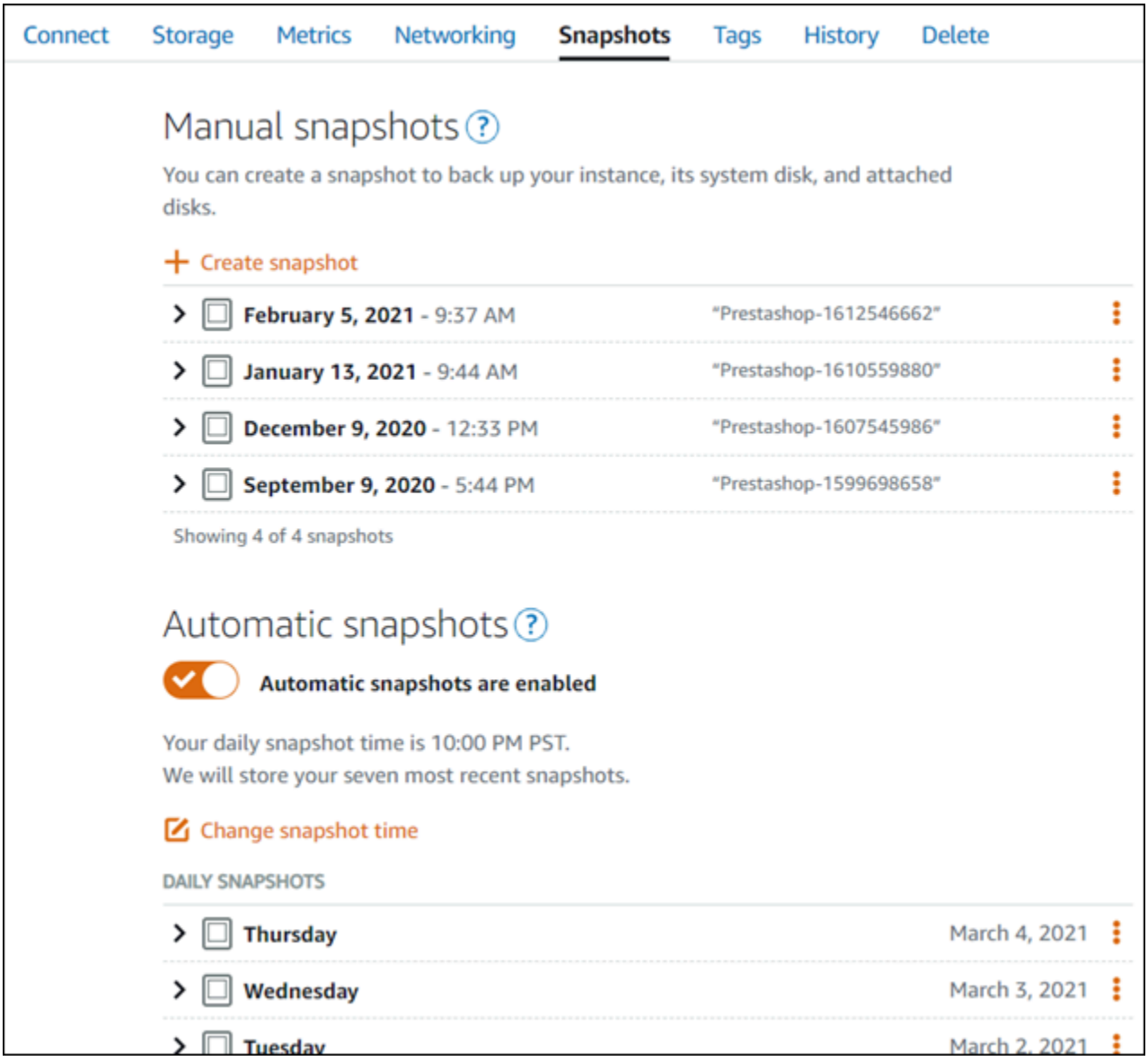
Schritt 7: Die WordPress-Multisite-Dokumentation lesen und Ihre Website weiter konfigurieren

Lesen Sie die WordPress-Multisite-Dokumentation, um zu erfahren, wie Sie Ihre Website verwalten und anpassen. Weitere Informationen finden Sie in der Netzwerkverwaltungs-Dokumentation für WordPress-Multisite.

Schritt 8: Einen Snapshot Ihrer Instance erstellen

Nachdem Sie Ihre WordPress-Multisite-Website so konfiguriert haben, wie Sie sie möchten, erstellen Sie periodische Snapshots Ihrer Instance, um diese zu sichern. Sie können Snapshots manuell erstellen oder automatische Snapshots aktivieren, damit Lightsail tägliche Snapshots für Sie erstellt.. Wenn etwas mit Ihrer Instance nicht stimmt, können Sie mit dem Snapshot eine neue Ersatz-Instance erstellen. Weitere Informationen finden Sie unter Snapshots.

Wählen Sie auf der Instance-Verwaltungsseite, unter der RegisterkarteSnapshotSnapshot erstellenoder wählen Sie aus, automatische Snapshots zu aktivieren.



Weitere Informationen finden Sie unter Erstellen eines Snapshots IhrerLinux- oder Unix-Instance inAmazon LightsailoderAktivieren oder Deaktivieren von automatischen Snapshots für Instances oder Datenträger inAmazon Lightsail.

Bitnami-Tutorials für Amazon Lightsail

Bitnami vereinfacht die Bereitstellung von Softwareanwendungen, indem es vorgefertigte und sofort einsatzbereite Entwicklungsstapel und Anwendungen für verschiedene Plattformen bereitstellt. Verwenden Sie die folgenden Tutorials, um zu erfahren, wie Sie mit Bitnami in Lightsail arbeiten.

Themen

- Abrufen des Anwendungs-Benutzernamens und des Passworts für Ihre Bitnami-Instance
- Entfernung des Bitnami-Banners von einer Bitnami-Vorlagen-Instance in Lightsail

Abrufen des Anwendungs-Benutzernamens und des Passworts für Ihre Bitnami-Instance

Bitnami stellt viele der Anwendungsinstance-Images oder Vorlagen zur Verfügung, die Sie als Amazon Lightsail-Instances erstellen können, die Ihre Virtual Private Server sind. Diese Vorlagen werden auf der Instance-Erstellungsseite in der Lightsail-Konsole als „Verpackt durch Bitnami“ bezeichnet.

Nachdem Sie eine Instance mit einer Bitnami-Vorlage erstellt haben, können Sie sich bei dieser Anwendung anmelden, um sie zu verwalten. Dazu müssen Sie den Standardbenutzernamen und das Standardpasswort für die auf der Instance laufenden Anwendung und/oder Datenbank erhalten. In diesem Artikel erfahren Sie, wie Sie die notwendigen Informationen erhalten, damit Sie sich anmelden und Lightsail-Instances verwalten können, die aus den folgenden Vorlagen erstellt wurden:

- WordPress-Blogging und Content Management-Anwendung
- WordPress Multisite Blogging und Content Management-Anwendung mit Unterstützung für mehrere Websites auf derselben Instance
- Django-Entwicklungsstack
- WordPress-Blogging- und Content-Management-Anwendung
- LAMP Entwicklungs-Stack (PHP 7)
- Node.js Entwicklungs-Stack
- Joomla Content Management Anwendung

- Magento E-Commerce-Anwendung
- MEAN Entwicklungs-Stack
- Drupal Content Management Anwendung
- GitLab CE Repository Anwendung
- Redmine-Projektmanagementanwendung
- Nginx (LEMP) Entwicklungs-Stack

Abrufen des standardmäßigen Bitnami Anwendungs- und Datenbank-Benutzernamens

Dies sind die Standard-Anwendungs- und Datenbank-Benutzernamen für Lightsail-Instances, die mit den Bitnami-Blaupausen erstellt wurden:

> **Note**
>
> Nicht alle Bitnami-Vorlagen beinhalten eine Anwendung oder eine Datenbank. Der Benutzername wird als nicht anwendbar (N/A) aufgeführt, wenn keine Anwendung oder Datenbank in der Vorlage enthalten ist.

- WordPress, einschließlich WordPress Multisite
  - Anwendungsbenutzername: `user`
  - Datenbankbenutzername: `root`
- PrestaShop
  - Anwendungsbenutzername: `user@example.com`
  - Datenbankbenutzername: `root`
- Django
  - Anwendungsbenutzername: N/A
  - Datenbankbenutzername: `root`
- Ghost
  - Anwendungsbenutzername: `user@example.com`
  - Datenbankbenutzername: `root`
- LAMP-Stack (PHP 5 und PHP 7)
  - Anwendungsbenutzername: N/A

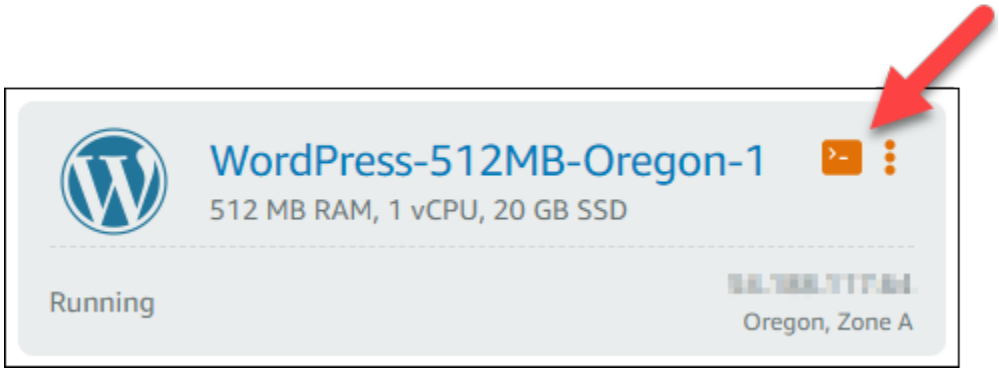
  - Datenbankbenutzername: `root`
- Node.js
  - Anwendungsbenutzername: N/A
  - Datenbankbenutzername: N/A
- Joomla
  - Anwendungsbenutzername: `user`
  - Datenbankbenutzername: `root`
- Magento
  - Anwendungsbenutzername: `user`
  - Datenbankbenutzername: `root`
- MEAN
  - Anwendungsbenutzername: N/A
  - Datenbankbenutzername: `root`
- Drupal
  - Anwendungsbenutzername: `user`
  - Datenbankbenutzername: `root`
- GitLab CE
  - Anwendungsbenutzername: `user`
  - Datenbankbenutzername: `postgres`
- Redmine
  - Anwendungsbenutzername: `user`
  - Datenbankbenutzername: `root`
- Nginx
  - Anwendungsbenutzername: N/A
  - Datenbankbenutzername: `root`

Abrufen des standardmäßigen Bitnami Anwendungs- und Datenbankpassworts

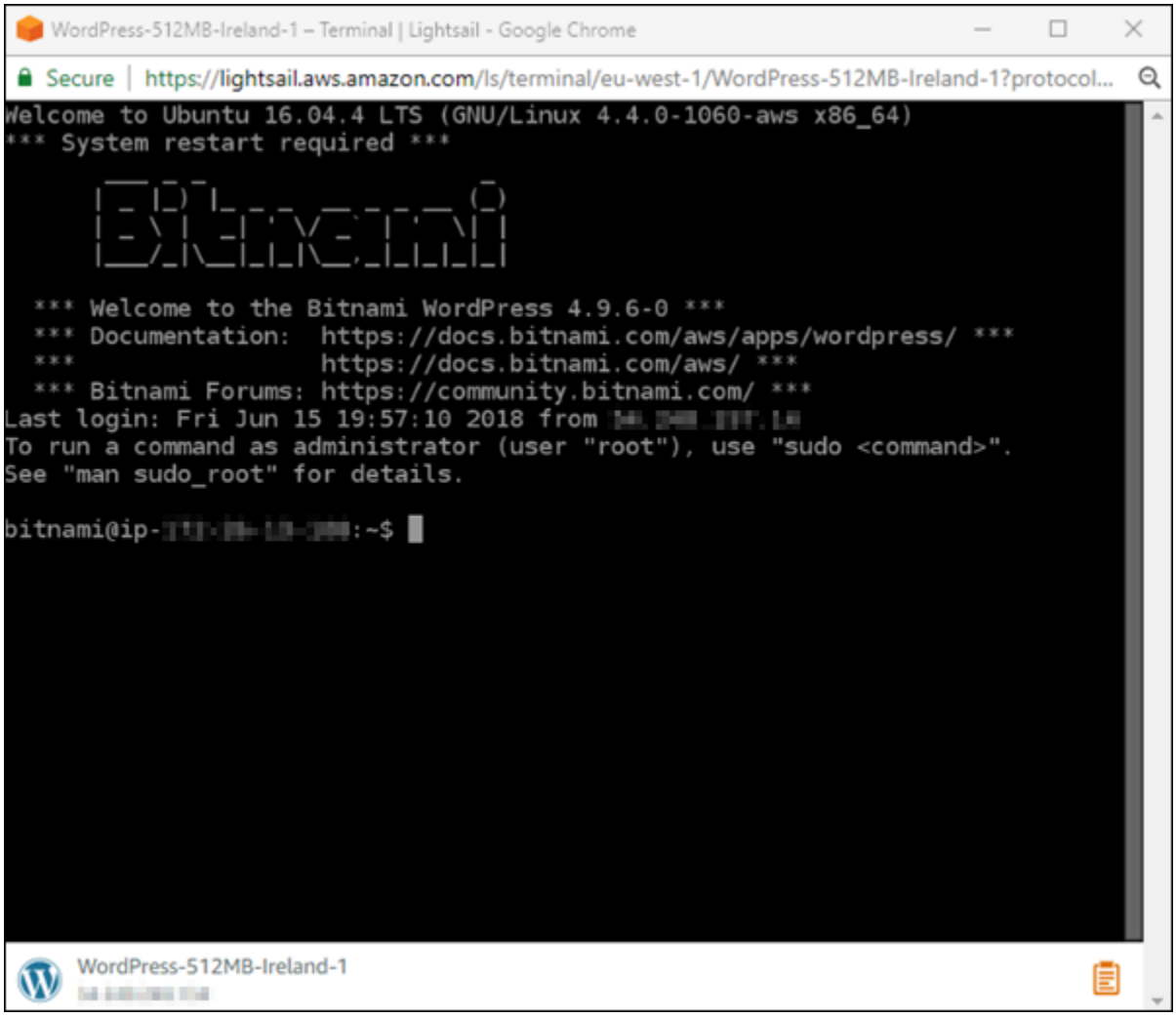
Die Standardanwendung und das Datenbankpasswort werden auf Ihrer Instance gespeichert. Sie rufen es ab, indem Sie sich mit Ihr über das browserbasierte SSH-Terminal in der Lightsail-Konsole verbinden und einen speziellen Befehl ausführen.

So rufen Sie das standardmäßige Bitnami Anwendungs- und Datenbankpasswort ab

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wenn Sie dies noch nicht getan haben, erstellen Sie eine Instance mit einer Bitnami-Vorlage. Weitere Informationen finden Sie unter Erstellen eines Amazon Lightsail-VPS.
3. Wählen Sie auf der Startseite von Lightsail das Schnellverbindungssymbol für die Instance, mit der Sie sich verbinden möchten.



Das browserbasierte SSH-Client-Fenster wird geöffnet, wie im folgenden Beispiel gezeigt.

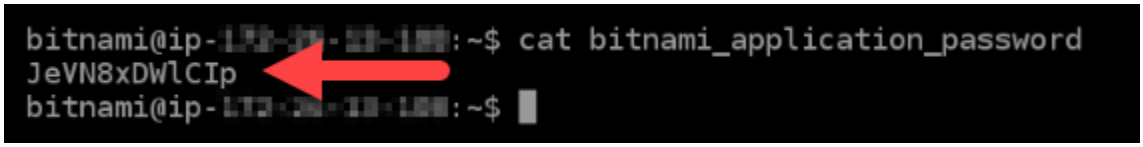


4. Geben Sie den folgenden Befehl ein, um das Standard-Anwendungspasswort abzurufen:

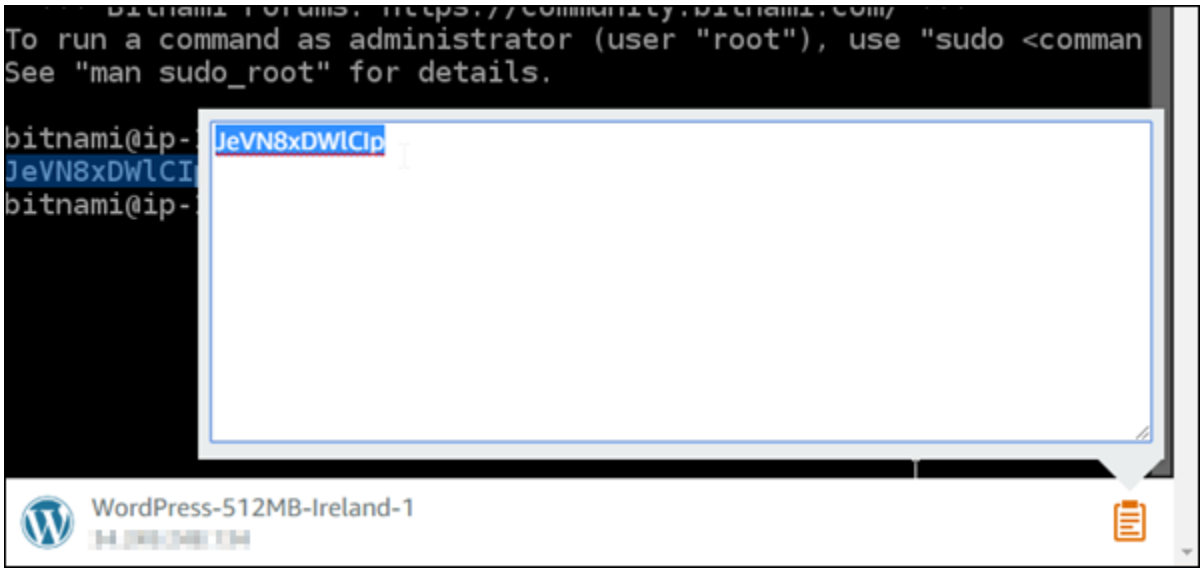
```
cat bitnami_application_password
```

> **Note**
>
> Wenn Sie sich in einem anderen Verzeichnis als dem Stammverzeichnis des Benutzers befinden, geben Sie `cat $HOME/bitnami_application_password` ein.

Sie sollten eine ähnliche Antwort wie diese sehen, die das Anwendungspasswort enthält:



5. Markieren Sie im Terminalbildschirm das Passwort und wählen Sie dann das Zwischenablagesymbol in der rechten unteren Ecke des browserbasierten SSH-Clientfensters.
6. Markieren Sie im Textfeld der Zwischenablage den Text, den Sie kopieren möchten, und drücken Sie dann Ctrl+C (STRG+C) oder Cmd+C, um den Text in Ihre lokale Zwischenablage zu kopieren.



> **Important**
>
> Achten Sie darauf, dass Sie Ihr Passwort zu diesem Zeitpunkt an irgendeinem Ort speichern. Sie können ihn später ändern, nachdem Sie sich bei der Bitnami-Anwendung auf Ihrer Instance angemeldet haben.

Melden Sie sich bei der Bitnami-Anwendung auf Ihrer Instance an

Melden Sie sich für Instances, die aus den Vorlagen von WordPress, Joomla, Magento, Drupal, GitLab CE und Redmine erstellt wurden, bei der Anwendung an, indem Sie zur öffentlichen IP-Adresse Ihrer Instance navigieren.

So melden Sie sich bei der Bitnami-Webanwendung an

1. Navigieren Sie in einem Browserfenster zur öffentlichen IP-Adresse Ihrer Instance.

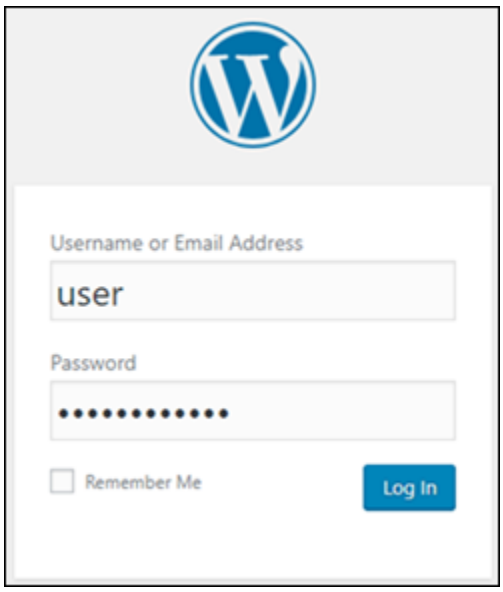
   Die Bitnami Anwendungs-Startseite wird geöffnet. Die Startseite wird entsprechend der Bitnami-Vorlage angezeigt, die Sie für Ihre Instance ausgewählt haben. Dies ist beispielsweise die WordPress-Anwendungsstartseite:

2. Wählen Sie das Bitnami-Logo in der rechten unteren Ecke der Anwendungshomepage, um zur Anwendungsinformationsseite zu gelangen.

> **Note**
>
> Die GitLab CE-Anwendung zeigt kein Bitnami-Logo an. Melden Sie sich stattdessen mit den Textfeldern Benutzername und Passwort an, die auf der Startseite von GitLab CE angezeigt werden.

Die Anwendungsinformationsseite enthält den Standardbenutzernamen und einen Link zur Anmeldeseite für die Anwendung auf Ihrer Instance.

3. Wählen Sie den Anmelde-Link auf der Seite, um zur Anmeldeseite für die Anwendung auf Ihrer Instance zu gelangen.
4. Geben Sie den Benutzernamen und das soeben erworbene Passwort ein und wählen Sie dann Log In (Anmelden).



Nächste Schritte

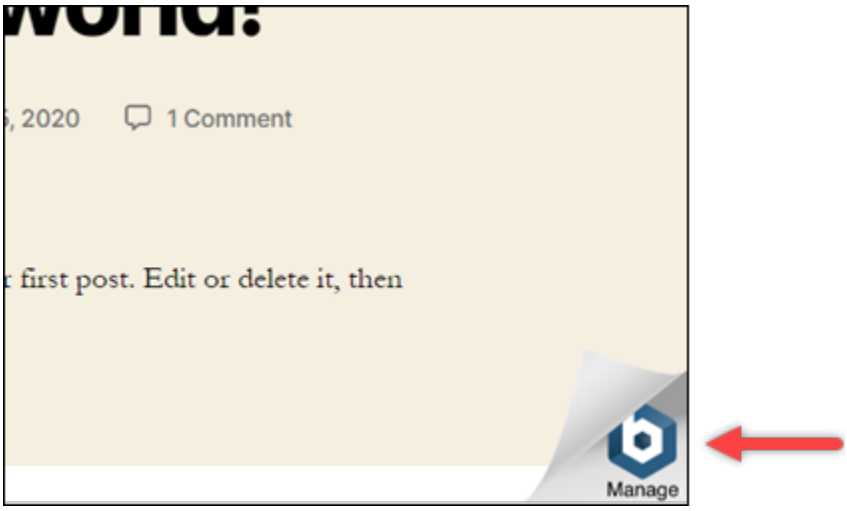
Verwenden Sie die folgenden Links, um mehr über die Bitnami-Vorlagen zu erfahren und sich die Tutorials anzusehen. Sie können beispielsweise Plug-ins installieren oder HTTPS-Support mit SSL-Zertifikaten für Ihre WordPress-Instance aktivieren.

- Bitnami WordPress für Amazon Web Services
- Bitnami LAMP-Stack für Amazon Web Services
- Bitnami Node.js für Amazon Web Services
- Bitnami Joomla für Amazon Web Services
- Bitnami Magento für Amazon Web Services
- Bitnami MEAN-Stack für Amazon Web Services
- Bitnami Drupal für Amazon Web Services
- Bitnami GitLab für Amazon Web Services
- Bitnami Redmine für Amazon Web Services
- Bitnami Nginx (LEMP-Stack) für Amazon Web Services

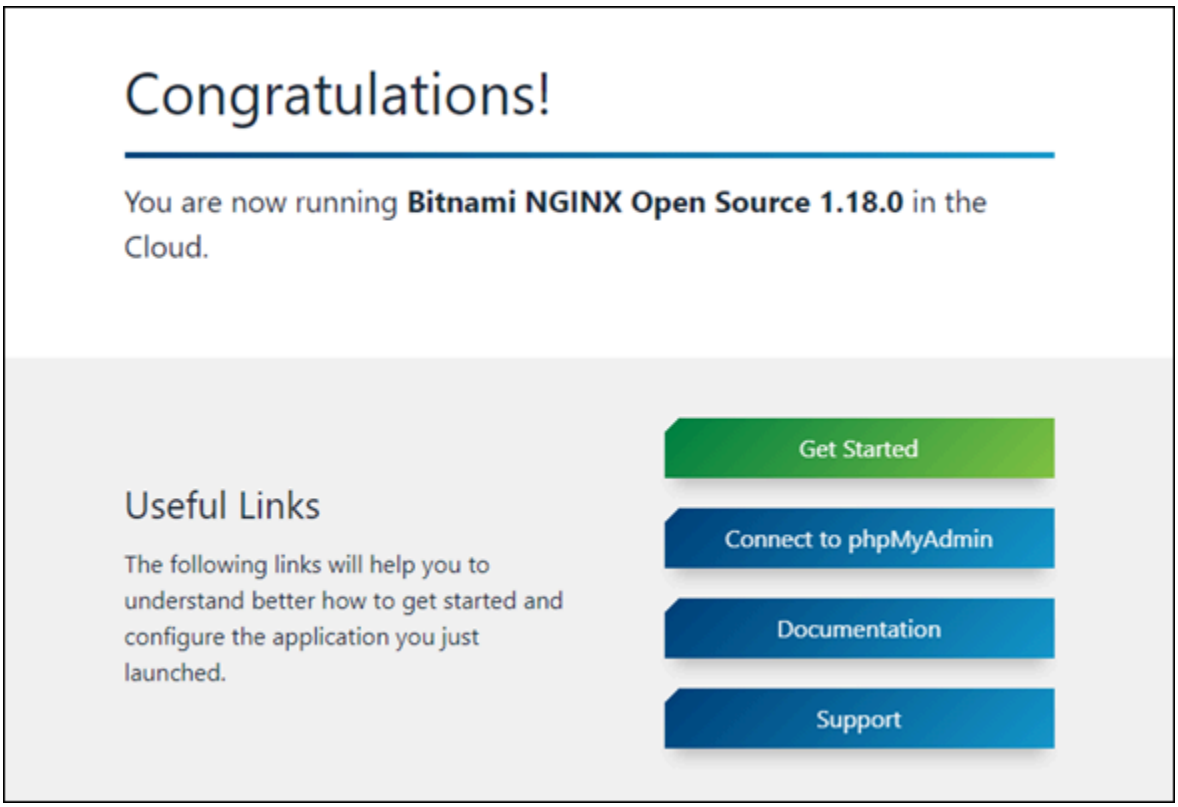
Weitere Informationen finden Sie unter Erste Schritte mit Bitnami-Anwendungen unter Verwendung von Amazon Lightsail oder Amazon Lightsail verwenden – Häufig gestellte Fragen.

Entfernung des Bitnami-Banners von einer Bitnami-Vorlagen-Instance in Lightsail

Einige der Bitnami-Vorlagen, die für Amazon Lightsail-Instances ausgewählt werden können, zeigen auf der Startseite der Anwendung ein Bitnami-Banner an. Im folgenden Beispiel aus einer „Certified by Bitnami“-WordPress-Instance wird das Bitnami-Banner in der unteren rechten Ecke der Homepage angezeigt. In diesem Leitfaden zeigen wir Ihnen, wie Sie das Bitnami-Symbol dauerhaft von der Startseite der Anwendung Ihrer Instance entfernen.



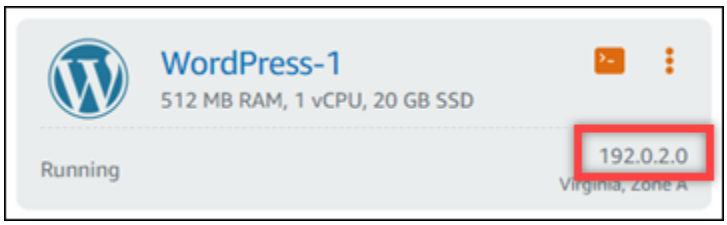
Nicht alle Bitnami-Vorlagenanwendungen zeigen das Bitnami-Banner auf der Startseite der Anwendung an. Besuchen Sie die Startseite IhrerLightsail-Instance, um festzustellen, ob ein Bitnami-Banner angezeigt wird. Im folgenden Beispiel einer „Verpackt von Bitnami“-Nginx-Instance wird das Bitnami-Symbol nicht angezeigt. Stattdessen wird eine Informationsseite für den Platzhalter angezeigt, die schließlich durch die Anwendung ersetzt wird, die Sie für die Instance bereitstellen möchten. Wenn Ihre Instance kein Bitnami-Banner anzeigt, müssen Sie die Anweisungen in diesem Leitfaden nicht befolgen.



Entfernen Sie das Bitnami-Banner aus Ihrer Instance

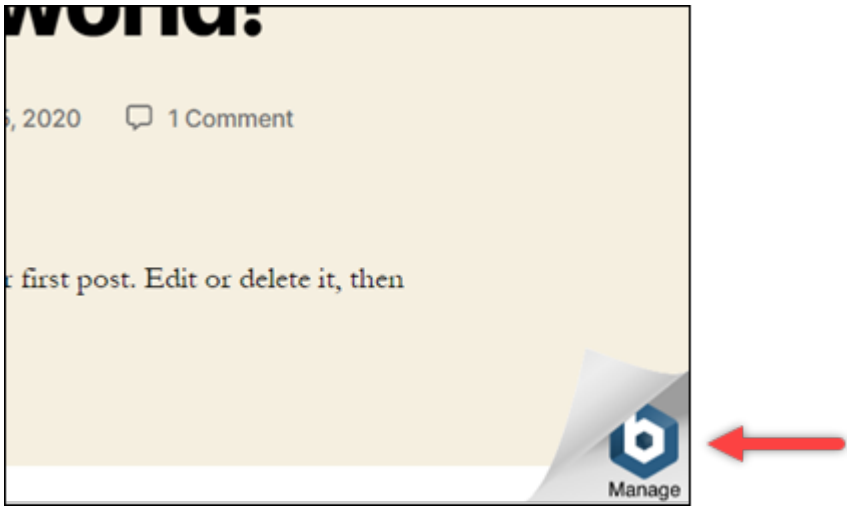
Führen Sie das folgende Verfahren aus, um zu bestätigen, dass auf der Startseite Ihrer Instance ein Bitnami-Symbol angezeigt wird und um es zu entfernen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Kopieren Sie in der Registerkarte Instances der Startseite Lightsail die öffentliche IP-Adresse der Instance, die Sie bestätigen möchten.

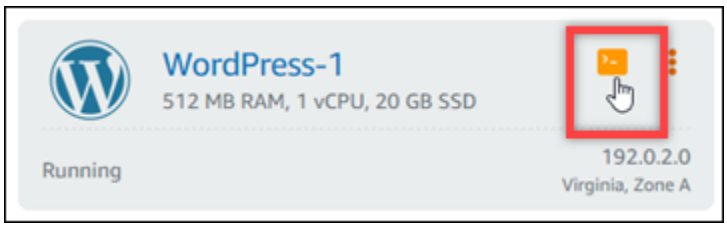


3. Öffnen Sie eine neue Browser-Registerkarte, geben Sie die öffentliche IP-Adresse Ihrer Instance in die Adressleiste ein und drücken SieEingabe.
4. Bestätigen Sie eine der folgenden Optionen:

   1. Wenn das Bitnami-Symbol auf der Seite nicht angezeigt wird, verfolgen Sie dieses Verfahren nicht weiter. Sie müssen das Bitnami-Symbol nicht von der Startseite Ihrer Anwendung entfernen.
   2. Wenn das Bitnami-Symbol in der rechten unteren Ecke der Seite angezeigt wird, wie im folgenden Beispiel gezeigt, fahren Sie mit den folgenden Schritten fort, um es zu entfernen.



   In den folgenden Schritten stellen Sie eine Verbindung mit Ihrer Instance her, indem Sie dieLightsailbrowserbasierter SSH-Client verwenden. Nachdem Sie eine Verbindung hergestellt haben, führen Sie das Bitnami Configuration Tool (bnconfig) aus, um das Bitnami-Symbol von der Startseite Ihrer Anwendung zu entfernen. Das bnconfig-Tool ist ein Befehlszeilen-Tool, mit dem Sie die Anwendung auf Ihrer Bitnami-Vorlagen-Instance konfigurieren können. Weitere Informationen finden Sie unterErfahren Sie mehr über das Bitnami Configuration Tool in der Bitnami-Dokumentation.
5. Kehren Sie zur Browser-Registerkarte zurück, die sich auf der Lightsail-Startseite befindet.
6. Wählen Sie das Symbol des browserbasierten SSH-Clients aus, das neben dem Namen der Instance angezeigt wird, mit der Sie sich verbinden möchten.



7. Nachdem der SSH-Client mit Ihrer Instance verbunden ist, geben Sie einen der folgenden Befehle ein:

   1. Wenn Ihre Instance Apache verwendet, geben Sie einen der folgenden Befehle ein. Wenn einer der Befehle fehlschlägt, versuchen Sie es mit dem anderen. Der erste Teil dieses Befehls deaktiviert das Bitnami-Banner und der zweite Teil startet den Apache-Dienst neu.

      ```
      sudo /opt/bitnami/apps/wordpress/bnconfig --disable_banner 1 && sudo /opt/
      bitnami/ctlscript.sh restart apache
      ```

      ```
      sudo /opt/bitnami/wordpress/bnconfig --disable_banner 1 && sudo /opt/bitnami/
      ctlscript.sh restart apache
      ```

   Sie können bestätigen, dass der Prozess erfolgreich war, indem Sie zur öffentlichen IP-Adresse Ihrer Instance navigieren und bestätigen, dass das Bitnami-Symbol verschwunden ist.

WordPress -Tutorials für Amazon Lightsail

WordPress ist ein Open-Source-Content-Management-System, mit dem Benutzer Websites und Blogs einfach erstellen und verwalten können. In den folgenden Tutorials erfahren Sie, wie Sie mit WordPress in Lightsail arbeiten.

Aufgaben

- Tutorial: Starten und konfigurieren Sie eine WordPress Instanz in Lightsail
- Tutorial: Verbinden einer WordPress-Website in Lightsail mit einem Amazon-S3-Bucket
- Tutorial: Verbinden einer WordPress-Instance in Lightsail mit einer Amazon-Aurora-Datenbank
- Tutorial: Verbinden Ihrer WordPress-Website mit einer MySQL-verwalteten Datenbank in Lightsail
- Tutorial: Verbinden einer WordPress Instance mit einem Lightsail-Bucket
- Konfigurieren Ihrer WordPress Instance für die Arbeit mit einer Netzwerkverteilung für die Bereitstellung von Inhalten in Lightsail

- Aktivieren Sie E-Mail auf Ihrer WordPress-Instance in Lightsail
- Aktivieren Sie HTTPS auf Ihrer WordPress Instanz in Lightsail
- Migrieren eines vorhandenen WordPress Blogs zu Amazon Lightsail

Tutorial: Starten und konfigurieren Sie eine WordPress Instanz in Lightsail

Amazon Lightsail ist der einfachste Weg, um mit Amazon Web Services (AWS) zu beginnen, wenn Sie nur Instances (virtuelle private Server) benötigen. Lightsail bietet alles, was Sie für einen schnellen Start Ihres Projekts benötigen — Instanzen, verwaltete Datenbanken, SSD-Speicher, Backups (Snapshots), Datenübertragung, Domain-DNS-Management, statische IPs und Load Balancer — zu einem niedrigen, vorhersehbaren Preis.

In diesem Tutorial erfahren Sie, wie Sie eine WordPress Instanz auf Lightsail starten und konfigurieren. Es umfasst Schritte zum Konfigurieren eines benutzerdefinierten Domainnamens, zum Sichern des Internetverkehrs mit HTTPS, zum Herstellen einer Verbindung mit Ihrer Instance mithilfe von SSH und zum Anmelden auf Ihrer Website. WordPress Wenn Sie mit diesem Tutorial fertig sind, verfügen Sie über die Grundlagen, um Ihre Instance auf Lightsail zum Laufen zu bringen.

> **Note**
>
> Im Rahmen des AWS kostenlosen Kontingents können Sie Amazon Lightsail für ausgewählte Instance-Pakete kostenlos nutzen. Weitere Informationen finden Sie unter AWS Kostenloses Kontingent auf der Preisseite von Amazon Lightsail.

Inhalt

Schritt 1: Melden Sie sich an für AWS

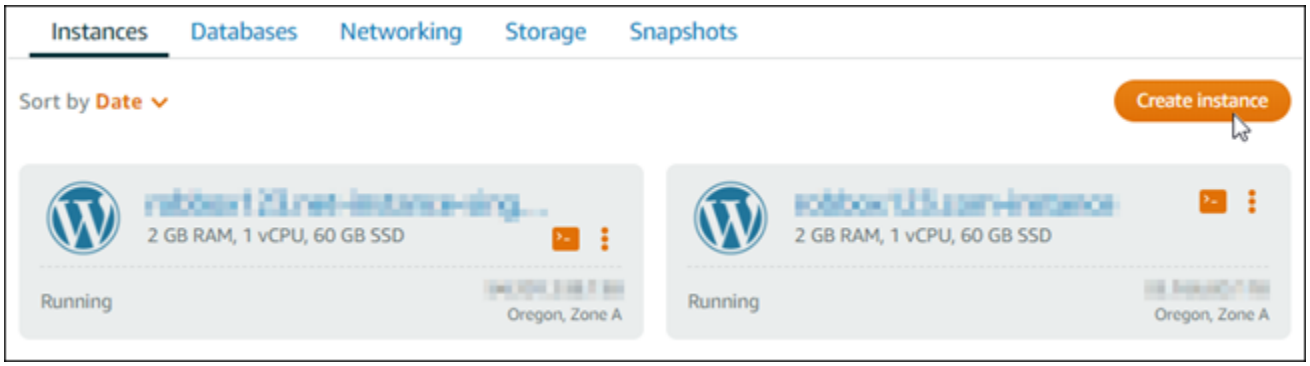
Amazon Lightsail benötigt eine. AWS-KontoMelden Sie sich an oder melden Sie sich an, AWS falls Sie bereits ein Konto haben. AWS

Schritt 2: Erstellen Sie eine WordPress Instanz

Führen Sie die folgenden Schritte aus, um Ihre WordPress Instance zum Laufen zu bringen. Weitere Informationen finden Sie unter the section called “Erstellen einer -Instance”.

So erstellen Sie eine Lightsail-Instanz für WordPress

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite im Abschnitt Instances die Option Create instance aus.



3. Wählen Sie die Availability Zone AWS-Region und die Availability Zone für Ihre Instance aus.

4. Wählen Sie das Image für Ihre Instanz wie folgt aus:

   a. Wählen Sie unter Plattform auswählen die Option Linux/Unix.

   b. Wählen Sie für Wählen Sie einen Blueprint aus. WordPress

5. Wählen Sie einen Instance-Plan.

   Ein Plan beinhaltet eine Maschinenkonfiguration (RAM, SSD, vCPU) zu niedrigen, vorhersehbaren Kosten sowie eine Datenübertragungsgebühr.

6. Geben Sie einen Namen für Ihre Instance ein. Ressourcennamen:

   - Muss AWS-Region in Ihrem Lightsail-Konto jeweils einzigartig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

7. Wählen Sie Create instance (Instance erstellen).

8. Um den Test-Blogbeitrag anzusehen, rufen Sie die Instanzverwaltungsseite auf und kopieren Sie die öffentliche IPv4-Adresse, die in der oberen rechten Ecke der Seite angezeigt wird. Fügen

Sie die Adresse in das Adressfeld eines mit dem Internet verbundenen Webbrowsers ein. Der Browser zeigt den Test-Blogbeitrag an.

Schritt 3: Konfigurieren Sie Ihre WordPress Instanz

Sie können Ihre WordPress Instanz mithilfe eines geführten step-by-step Workflows konfigurieren, oder Sie können die einzelnen Aufgaben ausführen. Mit einer der beiden Optionen konfigurieren Sie Folgendes:

- Ein registrierter Domainname — Ihre WordPress Website benötigt einen Domainnamen, den Sie sich leicht merken können. Benutzer geben diesen Domainnamen an, um auf Ihre WordPress Site zuzugreifen. Weitere Informationen finden Sie unter Domains und DNS.
- DNS-Verwaltung — Sie müssen entscheiden, wie Sie die DNS-Einträge für Ihre Domain verwalten möchten. Ein DNS-Eintrag teilt dem DNS-Server mit, welcher IP-Adresse oder welchem Hostnamen eine Domain oder Subdomain zugeordnet ist. Eine DNS-Zone enthält die DNS-Einträge für Ihre Domain. Weitere Informationen finden Sie unter the section called “DNS in Lightsail”.
- Eine statische IP-Adresse — Die öffentliche Standard-IP-Adresse für Ihre WordPress Instance ändert sich, wenn Sie Ihre Instance beenden und starten. Wenn Sie Ihrer Instance eine statische IP-Adresse zuordnen, bleibt sie auch dann unverändert, wenn Sie Ihre Instance beenden und starten. Weitere Informationen finden Sie unter the section called “IP-Adressen”.
- Ein SSL/TLS-Zertifikat — Nachdem Sie ein validiertes Zertifikat erstellt und es auf Ihrer Instance installiert haben, können Sie HTTPS für Ihre WordPress Website aktivieren, sodass der Datenverkehr, der über Ihre registrierte Domain an die Instance weitergeleitet wird, mit HTTPS verschlüsselt wird. Weitere Informationen finden Sie unter the section called “HTTPS aktivieren”.

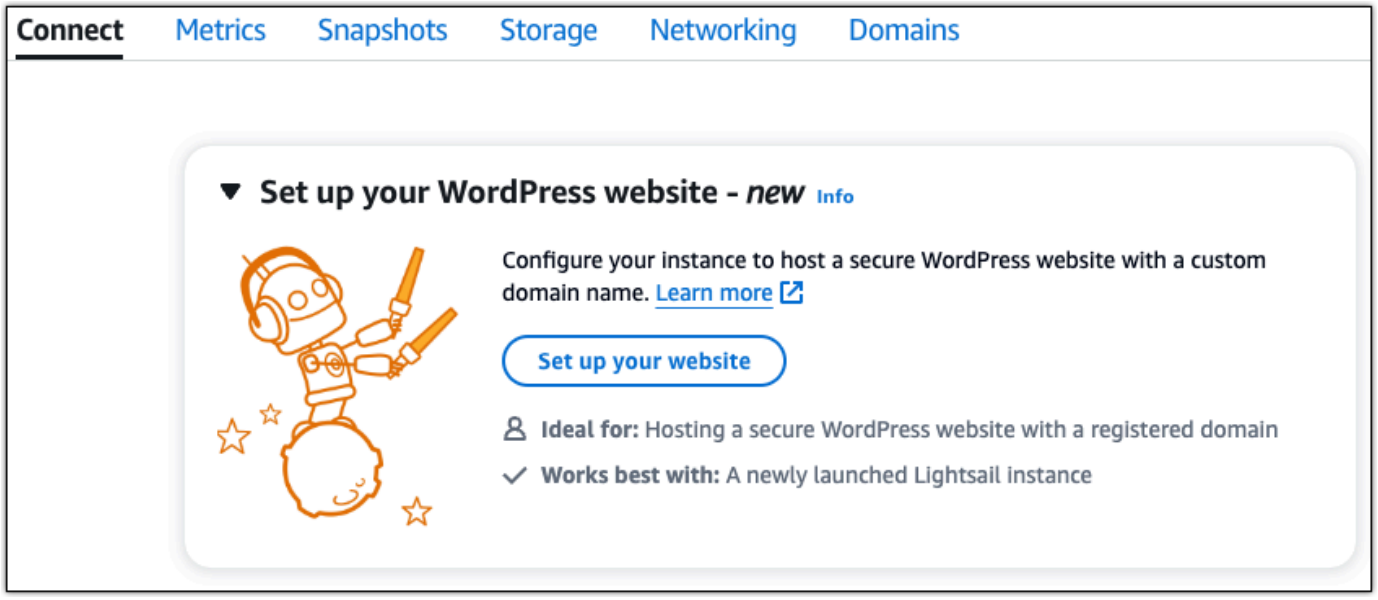
Option: Geführter Arbeitsablauf

> **Tip**
>
> Lesen Sie sich die folgenden Tipps durch, bevor Sie beginnen. Informationen zur Problembehandlung finden Sie unter Problembehandlung bei der WordPress Einrichtung.
>
> - Setup unterstützt Lightsail-Instanzen mit WordPress Version 6 und neuer, die nach dem 1. Januar 2023 erstellt wurden.

- Ihre Instanz muss sich im Status Running befinden. Warten Sie einige Minuten, bis die SSH-Verbindung bereit ist, falls die Instanz gerade gestartet wurde.
- Die Ports 22, 80 und 443 auf Ihrer Instance-Firewall müssen TCP-Verbindungen von jeder IP-Adresse aus zulassen, während das Setup läuft. Weitere Informationen finden Sie unter Instance-Firewalls.
- Wenn Sie DNS-Einträge hinzufügen oder aktualisieren, die auf Traffic von Ihrer Apex-Domain (`example.com`) und deren `www` Subdomänen (`www.example.com`) verweisen, müssen sie sich über das Internet verbreiten. Sie können überprüfen, ob Ihre DNS-Änderungen wirksam wurden, indem Sie Tools wie nslookup oder DNS Lookup from verwenden. MxToolbox
- WordPress-Instanzen, die vor dem 1. Januar 2023 erstellt wurden, enthalten möglicherweise ein veraltetes Certbot Personal Package Archive (PPA) -Repository, das dazu führt, dass die Einrichtung der Website fehlschlägt. Wenn dieses Repository während der Einrichtung vorhanden ist, wird es aus dem vorhandenen Pfad entfernt und an dem folgenden Speicherort auf Ihrer Instanz gesichert:. `~/opt/bitnami/lightsail/repo.backup` Weitere Informationen zum veralteten PPA finden Sie unter Certbot PPA auf der Canonical-Website.
- Let's Encrypt-Zertifikate werden automatisch alle 60 bis 90 Tage erneuert.
- Stoppen Sie Ihre Instanz nicht und nehmen Sie während des Setups keine Änderungen daran vor. Die Konfiguration Ihrer Instance kann bis zu 15 Minuten dauern. Sie können den Fortschritt für jeden Schritt auf der Registerkarte Instanzverbindung einsehen.

So konfigurieren Sie Ihre Instanz mit dem Website-Einrichtungsassistenten

1. Wählen Sie auf der Instanzverwaltungsseite auf dem Tab Connect die Option Website einrichten aus.



2. Verwenden Sie für Specify a domain name eine bestehende von Lightsail verwaltete Domain, registrieren Sie eine neue Domain bei Lightsail oder verwenden Sie eine Domain, die Sie über einen anderen Domain-Registrar registriert haben. Wählen Sie Diese Domain verwenden, um mit dem nächsten Schritt fortzufahren.
3. Führen Sie für Configure DNS einen der folgenden Schritte aus:
   - Wählen Sie von Lightsail verwaltete Domain, um eine Lightsail-DNS-Zone zu verwenden. Wählen Sie Diese DNS-Zone verwenden, um mit dem nächsten Schritt fortzufahren.
   - Wählen Sie Drittanbieter-Domain, um den Hosting-Dienst zu nutzen, der die DNS-Einträge für Ihre Domain verwaltet. Beachten Sie, dass wir eine passende DNS-Zone in Ihrem Lightsail-Konto erstellen, falls Sie diese später verwenden möchten. Wählen Sie DNS eines Drittanbieters verwenden, um mit dem nächsten Schritt fortzufahren.
4. Geben Sie unter Statische IP-Adresse erstellen einen Namen für Ihre statische IP-Adresse ein und wählen Sie dann Statische IP-Adresse erstellen aus.
5. Wählen Sie für Domainzuweisungen verwalten die Option Zuweisung hinzufügen, wählen Sie einen Domain-Typ und dann Hinzufügen aus. Wählen Sie Weiter, um mit dem nächsten Schritt fortzufahren.
6. Wählen Sie für Create an SSL/TLS certificate Ihre Domains und Subdomains aus, geben Sie eine E-Mail-Adresse ein, wählen Sie Ich autorisiere Lightsail, ein Let's Encrypt-Zertifikat auf meiner Instanz zu konfigurieren, und wählen Sie Zertifikat erstellen aus. Wir beginnen mit der Konfiguration der Lightsail-Ressourcen.

Stoppen Sie Ihre Instanz nicht und nehmen Sie während des Setups keine Änderungen daran vor. Die Konfiguration Ihrer Instance kann bis zu 15 Minuten dauern. Sie können den Fortschritt für jeden Schritt auf der Registerkarte Instanzverbindung einsehen.

7. Nachdem die Einrichtung der Website abgeschlossen ist, vergewissern Sie sich, dass die URLs, die Sie im Schritt Domainzuweisungen angegeben haben, Ihre WordPress Website öffnen.

Option: Einzelne Aufgaben

Um Ihre Instanz zu konfigurieren, indem Sie die einzelnen Aufgaben ausführen

1. Erstellen einer statischen IP-Adresse

   Wählen Sie auf der Seite zur Instanzverwaltung auf der Registerkarte Netzwerk die Option Statische IP erstellen aus. Der statische IP-Standort und die Instanz werden für Sie ausgewählt. Geben Sie einen Namen für Ihre statische IP-Adresse an und wählen Sie dann Create and attach.

2. Erstellen einer DNS-Zone

   Wählen Sie im Navigationsbereich Domains & DNS aus. Wählen Sie DNS-Zone erstellen, geben Sie Ihre Domain ein und wählen Sie dann DNS-Zone erstellen aus. Wenn derzeit Web-Traffic an Ihre Domain weitergeleitet wird, stellen Sie sicher, dass alle vorhandenen DNS-Einträge in der Lightsail-DNS-Zone vorhanden sind, bevor Sie die Nameserver beim aktuellen DNS-Hosting-Anbieter Ihrer Domain ändern. Auf diese Weise fließt der Verkehr nach der Übertragung in die Lightsail-DNS-Zone kontinuierlich und ununterbrochen

3. Domainzuweisungen verwalten

   Wählen Sie auf der Seite für die DNS-Zone auf der Registerkarte Zuweisungen die Option Zuweisung hinzufügen aus. Wählen Sie die Domain oder Subdomain, wählen Sie Ihre Instance aus, hängen Sie die statische IP-Adresse an und wählen Sie dann Zuweisen.

> **Tip**
>
> Warten Sie, bis sich diese Änderungen im Internet verbreiten, bevor Ihre Domain den Datenverkehr an Ihre Instance weiterleitet. WordPress

4. Erstellen und installieren Sie ein SSL/TLS-Zertifikat

   step-by-step Eine Anleitung finden Sie unter. the section called “HTTPS aktivieren”

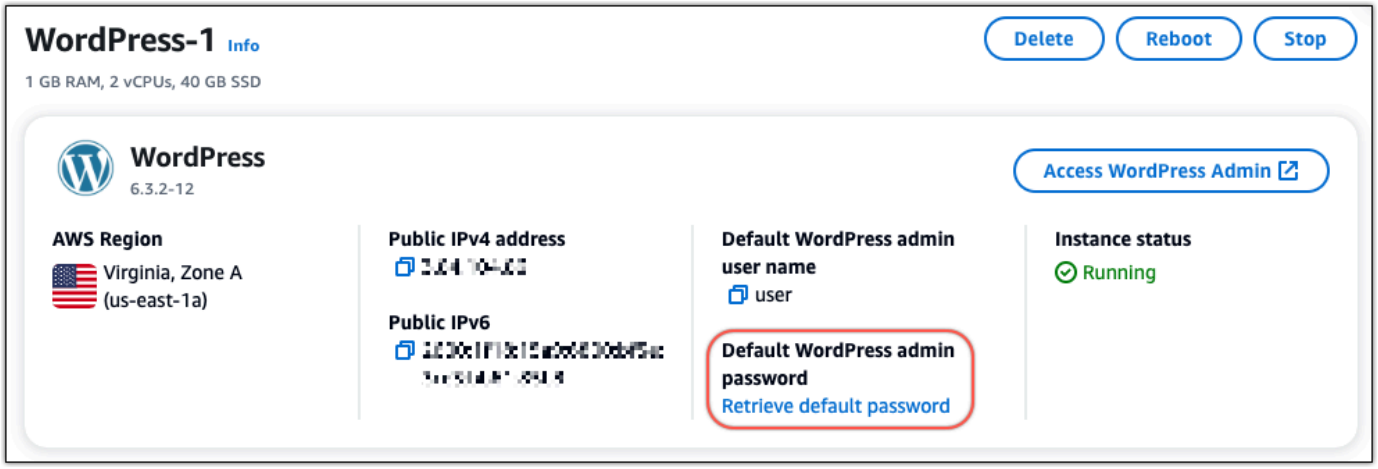
5. Vergewissern Sie sich, dass die URLs, die Sie im Schritt Domainzuweisungen angegeben haben, Ihre WordPress Site öffnen.

Schritt 4: Holen Sie sich das Admin-Passwort für Ihre WordPress Website

Das Standardpasswort für die Anmeldung im Administrations-Dashboard Ihrer WordPress Website ist auf der Instanz gespeichert. Führen Sie die folgenden Schritte aus, um das Passwort zu erhalten.

Um das Standardkennwort für den WordPress Administrator zu erhalten

1. Öffnen Sie die Instanzverwaltungsseite für Ihre WordPress Instanz.
2. Wählen Sie im WordPressPanel die Option Standardkennwort abrufen aus. Dadurch wird das Access-Standardkennwort unten auf der Seite erweitert.



3. Wählen Sie Launch. CloudShell Dadurch wird unten auf der Seite ein Fenster geöffnet.
4. Wählen Sie Kopieren und fügen Sie den Inhalt dann in das CloudShell Fenster ein. Sie können entweder den Cursor auf die CloudShell Eingabeaufforderung setzen und Strg+V drücken, oder Sie können mit der rechten Maustaste klicken, um das Menü zu öffnen, und dann Einfügen wählen.
5. Notieren Sie sich das im CloudShell Fenster angezeigte Passwort. Sie benötigen es, um sich im Administrations-Dashboard Ihrer WordPress Website anzumelden.

Schritt 5: Melden Sie sich im Administrations-Dashboard Ihrer Website an WordPress

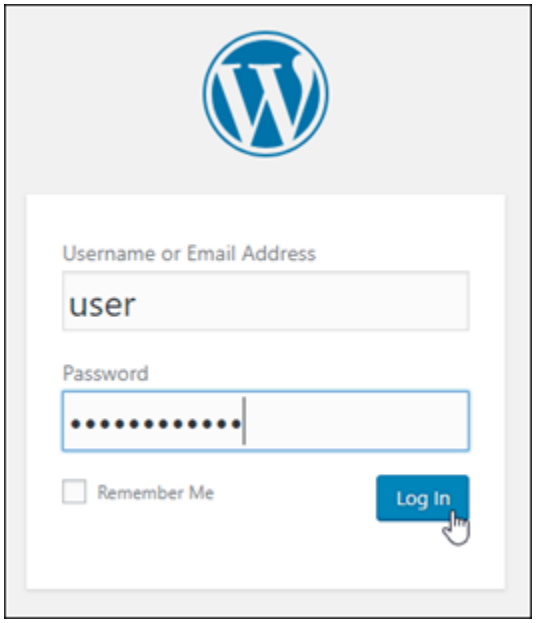
Nachdem Sie das Passwort für das Administrations-Dashboard Ihrer WordPress Website haben, können Sie sich anmelden. Im Verwaltungs-Dashboard können Sie Ihr Benutzerpasswort ändern, Plugins installieren, das Design Ihrer Website ändern und vieles mehr.

Führen Sie die folgenden Schritte aus, um sich im Administrations-Dashboard Ihrer WordPress Website anzumelden.

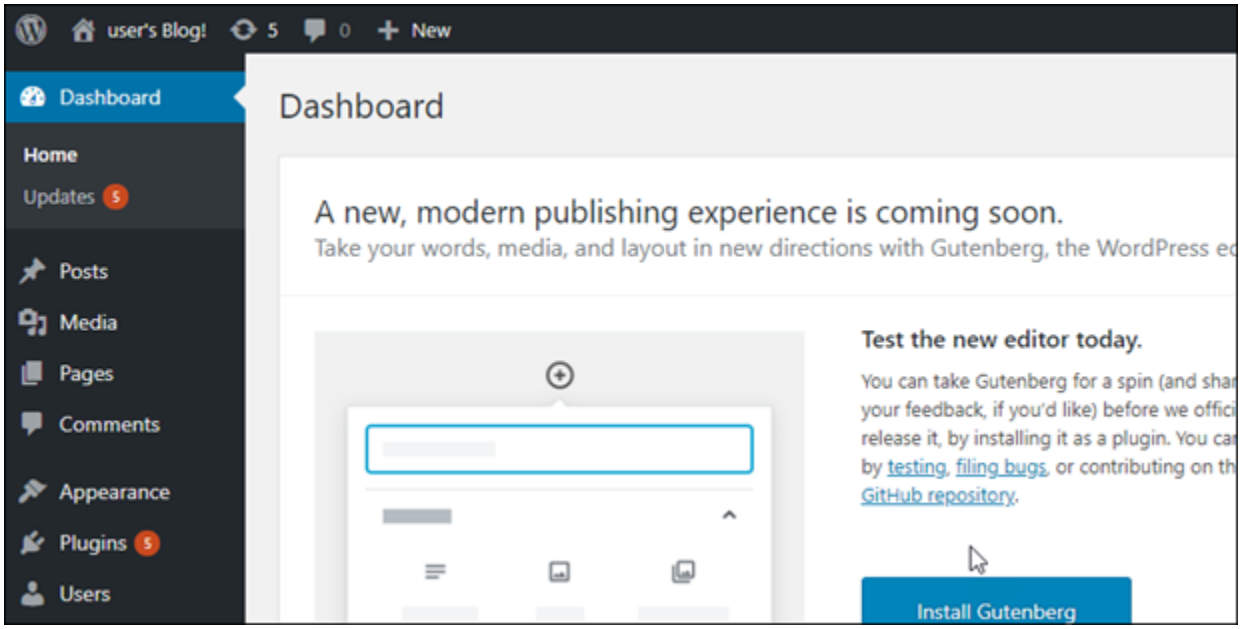
Um sich im Administrations-Dashboard anzumelden

1. Öffnen Sie die Instanzverwaltungsseite für Ihre WordPress Instanz.
2. Wählen Sie im WordPressPanel Access WordPress Admin aus.
3. Wählen Sie im Bereich Access your WordPress Admin Dashboard unter Öffentliche IP-Adresse verwenden den Link mit dem folgenden Format aus:

   http://*public-ipv4-Adresse*. /wp-admin
4. Geben Sie als Benutzername oder E-Mail-Adresse ein. **`user`**
5. Geben Sie unter Passwort das Passwort ein, das Sie im vorherigen Schritt erhalten haben.
6. Wählen Sie Log in (Anmelden).



Sie sind jetzt im Administrations-Dashboard Ihrer WordPress Website angemeldet, wo Sie administrative Aktionen ausführen können. Weitere Informationen zur Verwaltung Ihrer WordPress Website finden Sie im WordPressCodex in der WordPress Dokumentation.



Zusätzliche Informationen

Hier sind einige zusätzliche Schritte, die Sie nach dem Start einer WordPress Instance in Amazon Lightsail ausführen können:

- the section called “Konfigurieren eines CDN”
- Erstellen eines Snapshots Ihrer Linux-/Unix-basierten Instance
- Aktivieren oder Deaktivieren von automatischen Snapshots für Instances oder Datenträger
- Erstellen von zusätzlichen Blockspeicher-Datenträgern und Anfügen an Linux-basierte -Instances

Tutorial: Verbinden einer WordPress-Website in Lightsail mit einem Amazon-S3-Bucket

In diesem Tutorial werden die erforderlichen Schritte erläutert, um Ihre WordPress-Website, die auf einer Amazon Lightsail-Instance ausgeführt wird, mit einem Amazon Simple Storage Service (Amazon S3)-Bucket zu verbinden, um Website-Images und Anhänge zu speichern. Hierfür konfigurieren Sie ein WordPress-Plugin mit einer Reihe von Amazon Web Services (AWS)-Kontoanmeldeinformationen. Das Plugin erstellt dann den Amazon-S3-Bucket für Sie und konfiguriert Ihre Website so, dass sie für Website-Images und Anhänge den Bucket anstelle des Datenträgers der Instance verwendet.

Inhalt

Schritt 1: Erfüllen der Voraussetzungen

Bevor Sie beginnen, erstellen Sie eine WordPress-Instance in Lightsail und vergewissern Sie sich, dass diese ausgeführt wird. Weitere Informationen finden Sie im Tutorial: Starten und Konfigurieren einer WordPress-Instance.

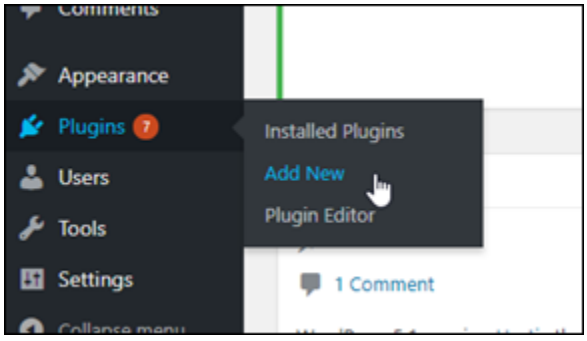
Schritt 2: Installieren des WP Offload Media-Plug-Ins auf Ihrer WordPress-Website

Sie müssen ein Plugin verwenden, um Ihre Website für die Verwendung eines Amazon-S3-Buckets zu konfigurieren. Für diese Konfiguration sind viele Plug-Ins verfügbar. Eines dieser Plug-Ins ist WP Offload Media Lite.

Führen Sie die folgenden Schritte aus, um das WP Offload Media-Plug-In auf Ihrer WordPress-Website zu installieren:

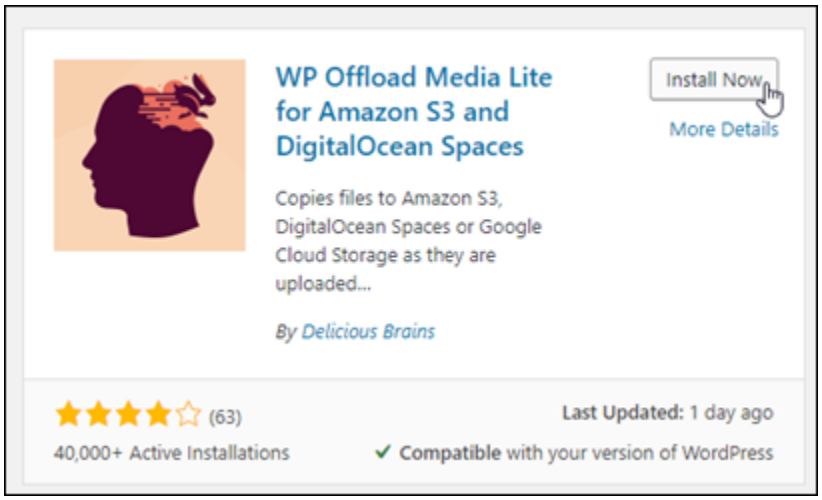
1. Melden Sie sich als Administrator bei Ihrem WordPress-Dashboard an.

   Weitere Informationen finden Sie unter Abrufen des Anwendungs-Benutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.
2. Bewegen Sie den Mauszeiger über Plug-Ins im linken Navigationsmenü und wählen Sie Add New (Neues auswählen) aus.



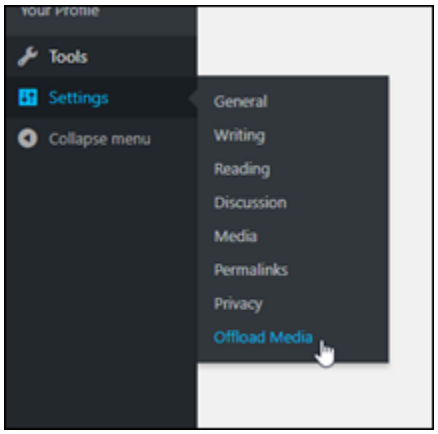
3. Suchen Sie nach WP Offload Media Lite.

4. Wählen Sie in den Suchergebnissen Install Now (Jetzt installieren) neben dem WP Offload Media-Plug-In aus.



5. Wählen Sie Activate (Aktivieren) aus, nachdem das Plug-In installiert wurde.

6. Wählen Sie im linken Navigationsmenü Settings (Einstellungen) und dann Offload Media aus.



7. Wählen Sie auf der Seite Offload Media Amazon S3 als Speicheranbieter und anschließend Zugriffsschlüssel in wp-config.php definieren aus.

   Bei dieser Option müssen Sie Ihre AWS-Kontoanmeldeinformationen zur Datei `wp-config.php` auf der Instance hinzufügen. Diese Schritte werden später in diesem Tutorial behandelt.

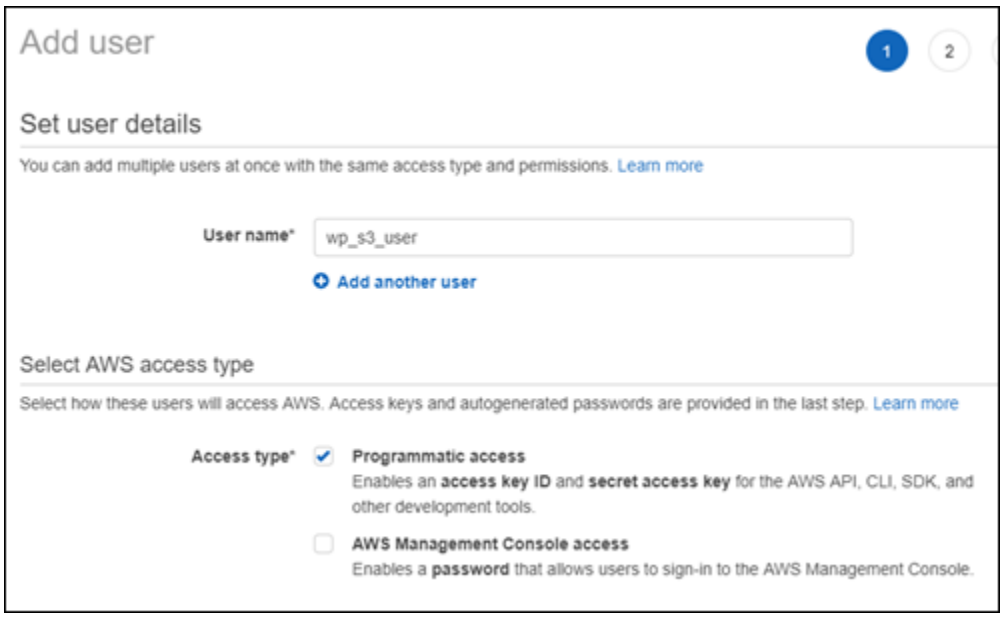
Lassen Sie die Seite Offload Media geöffnet. Sie werden später in diesem Tutorial dorthin zurückkehren. Fahren Sie mit Schritt 3: Erstellen eines IAM-Benutzers und einer Richtlinie in diesem Tutorial fort.

Schritt 3: Erstellen eines IAM-Benutzers und einer Richtlinie

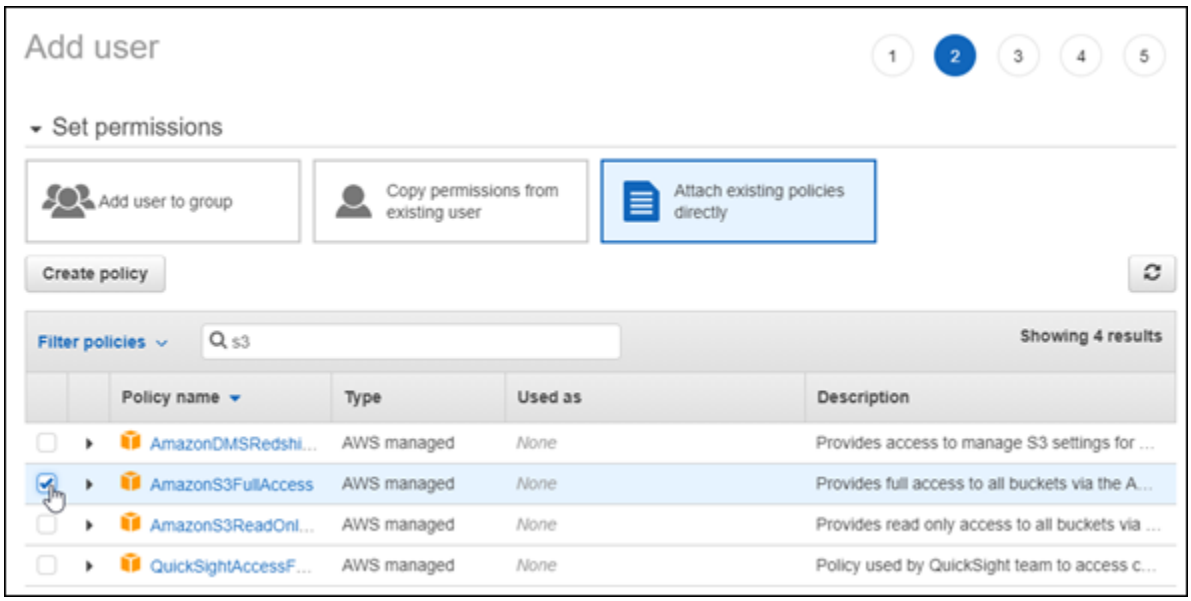
Das WP-Offload-Media-Plugin benötigt Zugriff auf Ihr AWS-Konto, um den Amazon-S3-Bucket zu erstellen und Ihre Website-Images und Anhänge hochzuladen.

Führen Sie die folgenden Schritte aus, um einen neuen AWS Identity and Access Management (IAM)-Benutzer und eine neue Richtlinie für das WP-Offload-Media-Plugin zu erstellen:

1. Öffnen Sie eine neue Browser-Registerkarte und melden Sie sich bei der IAM-Konsole an.
2. Wählen Sie im linken Navigationsmenü auf Users (Benutzer) aus.
3. Wählen Sie Benutzer hinzufügen.
4. Geben Sie in das Textfeld User name (Benutzername) einen Namen für den neuen Benutzer ein. Geben Sie eine Beschreibung ein, z. B. `wp_s3_user` oder `wp_offload_media_plugin_user`, um eine leichtere Identifizierung bei zukünftigen Wartungsarbeiten zu ermöglichen.
5. Wählen Sie im Abschnitt Access type (Zugriffstyp) die Option Programmatic access (Programmgesteuerter Zugriff) aus.



6. Wählen Sie Next: Permissions (Weiter: Berechtigungen) aus.
7. Wählen Sie Attach existing policies directly (Vorhandene Richtlinien direkt anfügen) aus, suchen Sie nach S3 und wählen Sie dann AmazonS3FullAccess in den Suchergebnissen aus.



8. Wählen Sie Next: Tags (Weiter: Tags) und danach Next: Review (Weiter: Prüfen) aus.
9. Überprüfen Sie die auf der Seite angezeigten Benutzerdetails und wählen Sie dann Create user (Benutzer erstellen) aus.
10. Notieren Sie sich die Zugriffsschlüssel-ID (Access Key ID) und den geheimen Zugriffsschlüssel (Secret Access Key) für den Benutzer oder wählen Sie Download .csv (.csv herunterladen) aus, um eine Kopie dieser Werte auf Ihrem lokalen Laufwerk zu speichern. Sie benötigen diese Werte

in den nächsten Schritten, wenn Sie die Datei `wp-config.php` auf der WordPress-Instance bearbeiten.

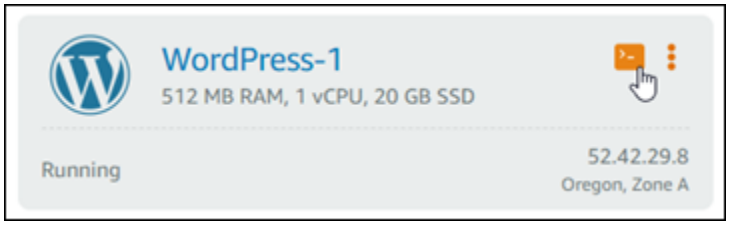
Schritt 4: Bearbeiten der WordPress-Konfigurationsdatei

Führen Sie die folgenden Schritte aus, um eine Verbindung zu Ihrer WordPress-Instance über den Browser-basierten SSH-Client in der Lightsail-Konsole herzustellen und die Datei `wp-config.php` zu bearbeiten.

Die Datei `wp-config.php` enthält die Basiskonfigurationsdetails Ihrer Website, beispielsweise Datenbankverbindungsinformationen.

> **Note**
>
> Für die Verbindung zu Ihrer Instance können Sie auch Ihren eigenen SSH-Client verwenden. Weitere Informationen finden Sie unter PuTTY herunterladen und einrichten, um eine Verbindung über SSH in Amazon Lightsail herzustellen

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie das Symbol des browserbasierten SSH-Clients für die WordPress-Instance aus.



3. Geben Sie im angezeigten SSH-Client-Fenster den folgenden Befehl ein, um eine Sicherung der Datei `wp-config.php` für den Fall eines Fehlers zu erstellen:

```
sudo cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-
config.php.backup
```

4. Geben Sie den folgenden Befehl ein, um die Datei `wp-config.php` mit `nano`, einem Texteditor, zu öffnen:

```
nano /opt/bitnami/wordpress/wp-config.php
```

5. Geben Sie den folgenden Text über dem Text `/* That's all, stop editing! Happy blogging. */` ein.

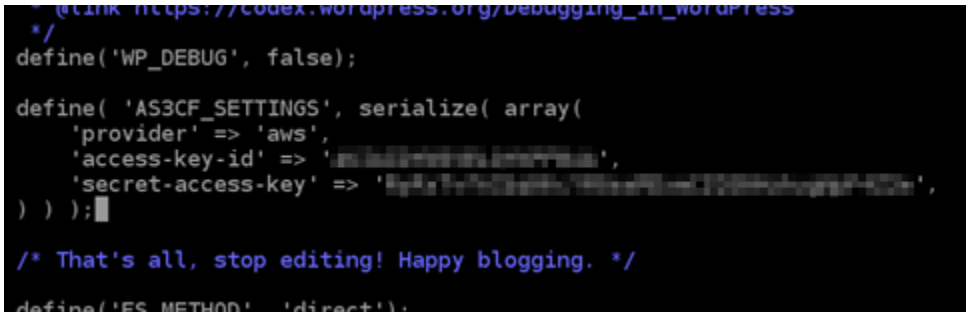
   Stellen Sie sicher, dass Sie *`AccessKeyID`* durch die Zugriffsschlüssel-ID und *`SecretAccessKey`* durch den geheimen Zugriffsschlüssel des IAM-Benutzers ersetzen, den Sie zuvor in diesen Schritten erstellt haben.

   ```
   define( 'AS3CF_SETTINGS', serialize( array(
       'provider' => 'aws',
       'access-key-id' => 'AccessKeyID',
       'secret-access-key' => 'SecretAccessKey',
   ) ) );
   ```

   Beispiel:

   ```
   define( 'AS3CF_SETTINGS', serialize( array(
       'provider' => 'aws',
       'access-key-id' => 'AKIAIOSFODNN7EXAMPLE',
       'secret-access-key' => 'wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY',
   ) ) );
   ```

   Das Ergebnis sollte wie folgt aussehen:

6. Drücken Sie **`Ctrl+X`**, um Nano zu beenden, und drücken Sie dann **`Y`** und **`Enter`**, um Ihre Änderungen an der Datei `wp-config.php` zu speichern.
7. Geben Sie den folgenden Befehl ein, um die Services auf der Instance neu zu starten:

   ```
   sudo /opt/bitnami/ctlscript.sh restart
   ```

   Nach dem Neustart der Services wird ein etwa wie folgt aussehendes Ergebnis angezeigt:

```
bitnami@ip-172-26-13-236:~$ sudo /opt/bitnami/ctlscript.sh restart
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd stopped
/opt/bitnami/php/scripts/ctl.sh : php-fpm stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql  started at port 3306
/opt/bitnami/php/scripts/ctl.sh : php-fpm started
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd started at port 80
bitnami@ip-172-26-13-236:~$
```

Schließen Sie das SSH-Fenster und wechseln Sie zurück zur Seite Offload Media, die Sie zuvor in diesem Tutorial geöffnet haben. Sie können nun den Amazon-S3-Bucket mithilfe des WP-Offload-Media-Plugins erstellen.

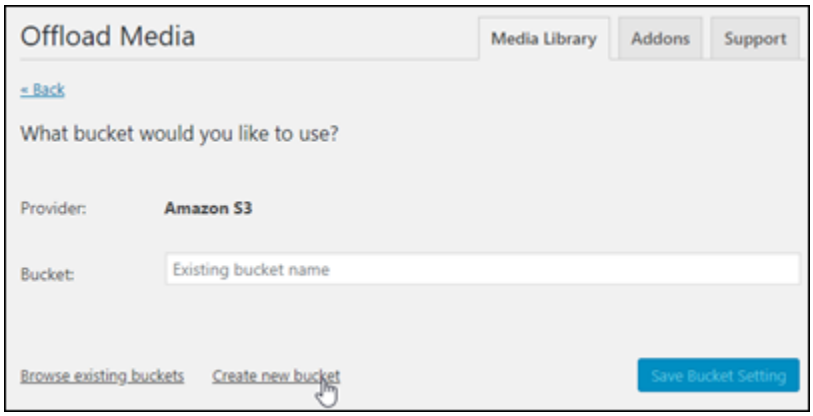
Schritt 5: Erstellen des Amazon S3-Buckets mithilfe des WP Offload Media-Plug-Ins

Nachdem die Datei `wp-config.php` nun mit den AWS-Anmeldeinformationen konfiguriert wurde, können Sie zur Seite Offload Media zurückkehren, um den Vorgang abzuschließen.

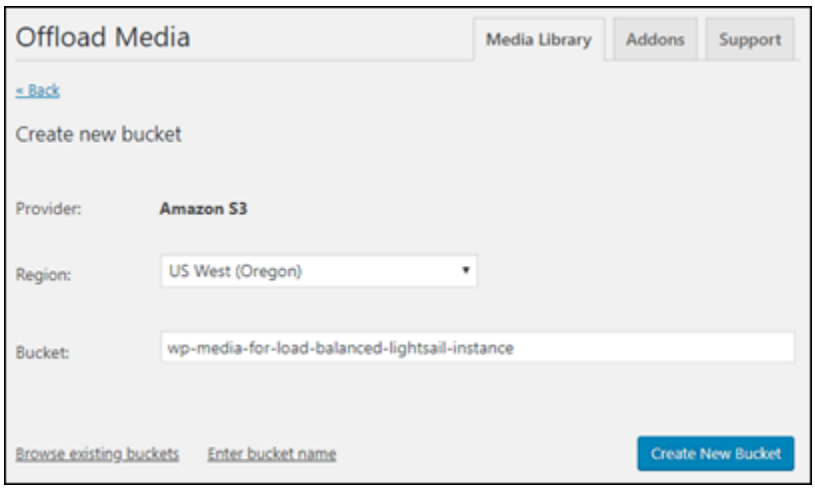
Führen Sie die folgenden Schritte aus, um den Amazon S3-Bucket mithilfe des WP Offload Media-Plug-Ins zu erstellen.

1. Aktualisieren Sie die Seite Offload Media oder wählen Sie Next (Weiter) aus.

   Es sollte jetzt zu sehen sein, dass der Amazon-S3-Anbieter konfiguriert ist.
2. Wählen Sie Create new bucket (Neuen Bucket erstellen) aus.

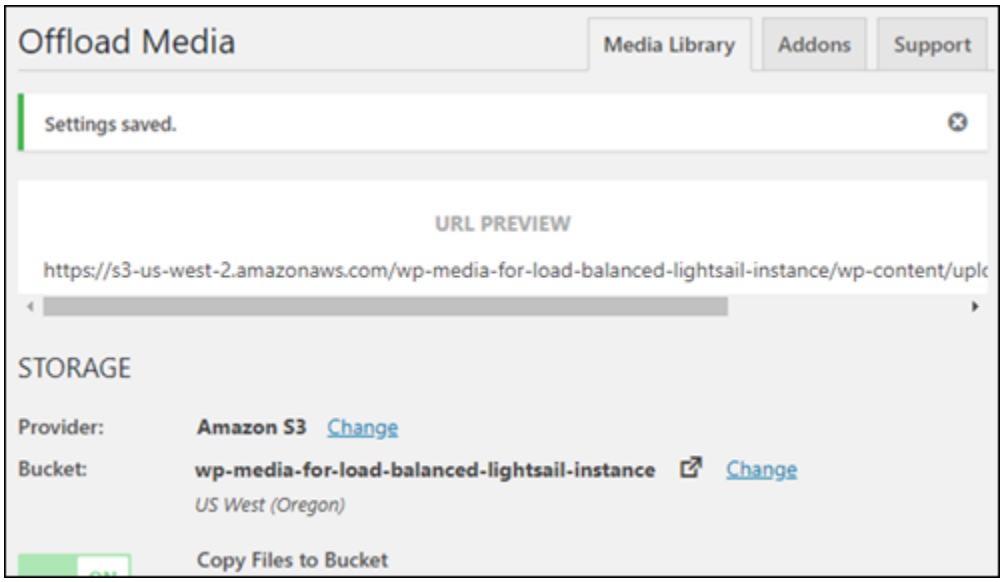


3. Wählen Sie im Dropdown-Menü Region die gewünschte AWS-Region aus. Wir empfehlen, die Region auszuwählen, in der sich Ihre WordPress-Instance befindet.
4. Geben Sie in das Textfeld Bucket einen Namen für den neuen S3-Bucket ein.



5. Wählen Sie Create New Bucket (Neuen Bucket erstellen) aus.

   Die Seite wird aktualisiert, um zu bestätigen, dass ein neuer Bucket erstellt wurde. Überprüfen Sie die angezeigten Einstellungen und passen Sie sie dem gewünschten Verhalten Ihrer WordPress-Website entsprechend an.



   Von nun an werden Images und Anhänge, die Blog-Beiträgen hinzugefügt wurden, automatisch in den von Ihnen erstellten Amazon-S3-Bucket hochgeladen.

Schritt 6: Nächste Schritte

Nachdem Sie die Verbindung Ihrer WordPress-Website mit einem Amazon-S3-Bucket abgeschlossen haben, sollten Sie einen Snapshot Ihrer WordPress-Instance erstellen, um die vorgenommenen

Änderungen zu sichern. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Linux- oder Unix-Instance.

Tutorial: Verbinden einer WordPress-Instance in Lightsail mit einer Amazon-Aurora-Datenbank

Die Daten der Website für Beiträge, Seiten und Benutzer werden in einer Datenbank gespeichert, die auf Ihrer WordPress-Instance in Amazon Lightsail ausgeführt wird. Wenn die WordPress-Instance ausfällt, können Sie Ihre Daten möglicherweise nicht wiederherstellten. Um dieses Szenario zu vermeiden, sollten Sie Ihre Websitedaten in eine Amazon-Aurora-Datenbank in Amazon Relational Database Service (Amazon RDS) übertragen.

Amazon Aurora ist eine mit MySQL und PostgreSQL kompatible relationale Datenbank, die für die Cloud entwickelt wurde. Sie kombiniert die Leistung und Verfügbarkeit traditioneller Unternehmensdatenbanken mit der Einfachheit und Kosteneffizienz von Open-Source-Datenbanken. Aurora wird als Teil von Amazon RDS angeboten. Amazon RDS ist ein verwalteter Datenbakservice, der das Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der Cloud vereinfacht. Weitere Informationen finden Sie im Benutzerhandbuch für Amazon Relational Database Service und im Benutzerhandbuch für Amazon Aurora.

In diesem Tutorial zeigen wir Ihnen, wie Sie Ihre Website-Datenbank von einer WordPress-Instance in Lightsail mit einer von Aurora verwalteten Datenbank in Amazon RDS verbinden.

Inhalt

Schritt 1: Erfüllen der Voraussetzungen

Stellen Sie vor Beginn sicher, dass die folgenden Voraussetzungen erfüllt sind:

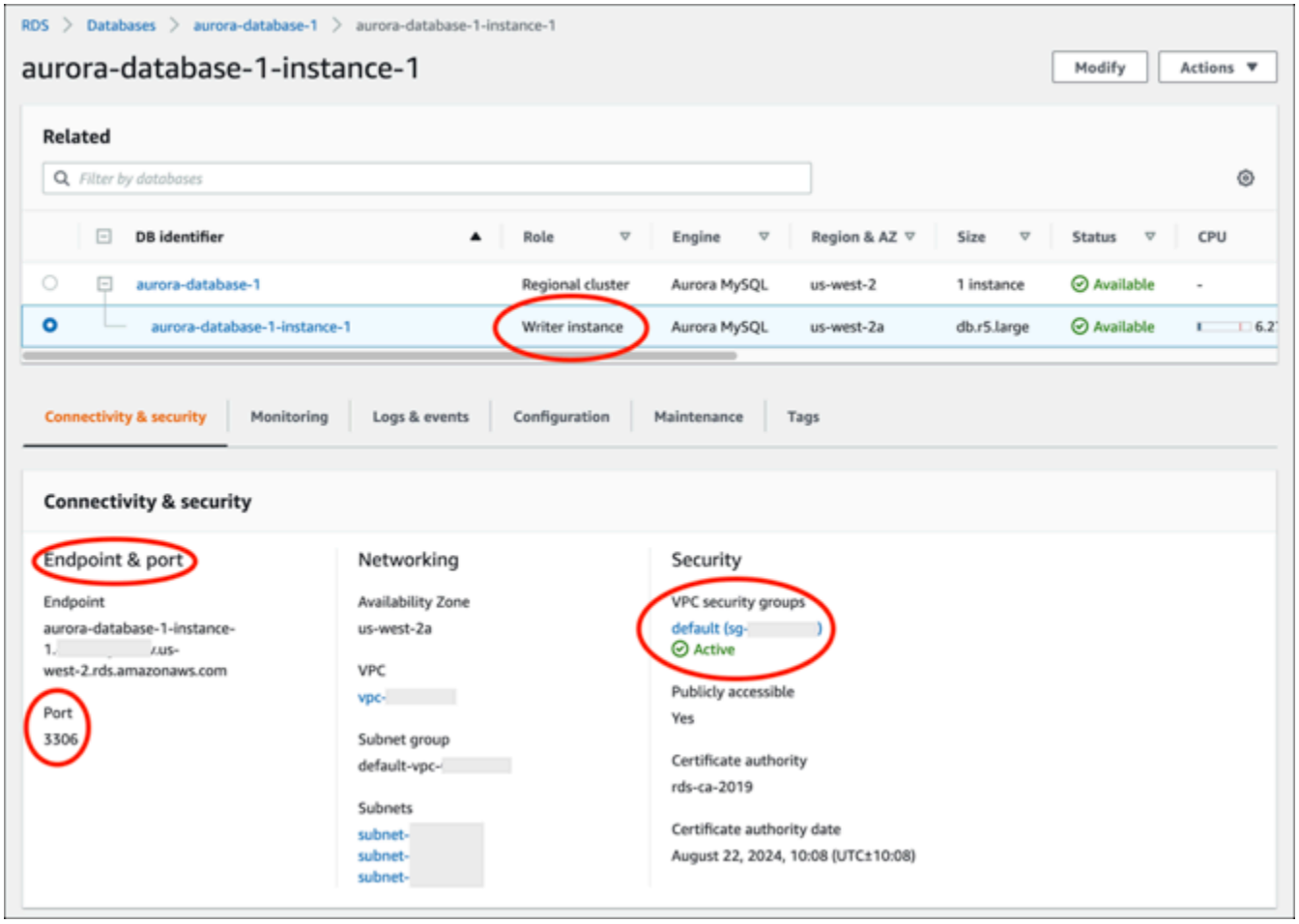
1. Erstellen Sie eine WordPress-Instance in Lightsail und konfigurieren Sie Ihre Anwendung darauf. Die Instance muss sich im laufenden Zustand befinden, bevor Sie fortfahren. Weitere Informationen finden Sie im Tutorial: Starten und Konfigurieren einer WordPress-Instance in Amazon Lightsail.
2. Aktivieren Sie in Ihrem Lightsail-Konto das VPC-Peering. Weitere Informationen finden Sie unter Einrichten von Peering für die Zusammenarbeit mit AWS-Ressourcen außerhalb von Lightsail.
3. Erstellen einer von Aurora verwalteten Datenbank in Amazon RDS. Die Datenbank muss sich in derselben AWS-Region wie Ihre WordPress-Instance befinden. Sie muss sich auch im laufenden Zustand befinden, bevor Sie fortfahren. Weitere Informationen finden Sie unter Erste Schritte mit Amazon Aurora im Amazon-Aurora-Benutzerhandbuch.

Schritt 2: Konfigurieren der Sicherheitsgruppe für Ihre Aurora-Datenbank

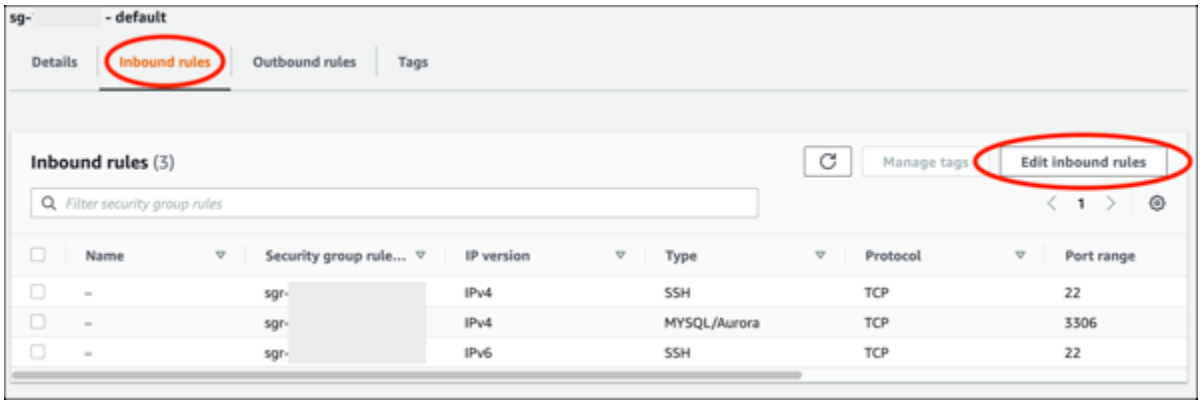
Eine AWS-Sicherheitsgruppe fungiert als virtuelle Firewall für Ihre AWS-Ressourcen. Sie kontrolliert den ein- und ausgehenden Datenverkehr, der sich mit Ihrer Aurora-Datenbank in Amazon RDS verbinden kann. Weitere Informationen finden Sie unter Kontrollieren des Datenverkehrs zu Ressourcen mithilfe von Sicherheitsgruppen im Benutzerhandbuch von Amazon Virtual Private Cloud.

Führen Sie das folgende Verfahren aus, um die Sicherheitsgruppe so zu konfigurieren, dass Ihre WordPress-Instance eine Verbindung zu Ihrer Aurora-Datenbank herstellen kann.

1. Melden Sie sich bei der Amazon-RDS-Konsole an.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie das Symbol der Writer-Instance der -Datenbank aus, mit der Ihre WordPress-Instance eine Verbindung herstellen wird.
4. Wählen Sie die Registerkarte Connectivity & security (Konnektivität und Sicherheit).
5. Notieren Sie sich aus dem Abschnitt Endpoint & Port (Endpunkt und Port) den Endpoint name (Endpunktnamen) und den Port (Port) der Writer-Instance. Sie benötigen diese Angaben später bei der Konfiguration Ihrer Lightsail-Instance zur Verbindungsherstellung mit der Datenbank.
6. Wählen Sie im Bereich Security (Sicherheit) den Link der aktiven VPC-Sicherheitsgruppe aus. Sie werden zur Sicherheitsgruppe Ihrer Datenbank weitergeleitet.



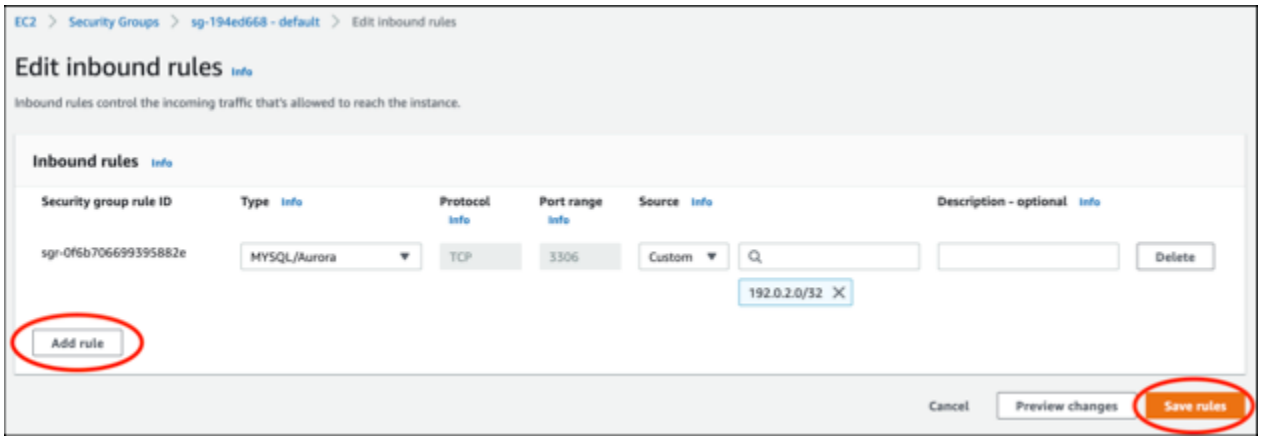
7. Vergewissern Sie sich, dass die Sicherheitsgruppe für Ihre Aurora-Datenbank ausgewählt ist.
8. Wählen Sie die Registerkarte Inbound rules (Regeln für eingehenden Datenverkehr) aus.
9. Wählen Sie Edit inbound rules (Regeln für eingehenden Datenverkehr bearbeiten) aus.



10. Wählen Sie auf der Seite Edit inbound rules (Regeln für eingehenden Datenverkehr bearbeiten) die Option Add Rule (Regel hinzufügen).
11. Führen Sie die folgenden Schritte aus:

- Wenn Sie den standardmäßigen MySQL-Port 3306 verwenden, wählen Sie MySQL/Aurora im Dropdownmenü Type (Typ) aus.
- Wenn Sie einen benutzerdefinierten Port für Ihre Datenbank verwenden, wählen Sie Custom TCP(Benutzerdefiniertes TCP) im Dropdownmenü Type (Typ) aus und geben Sie im Textfeld Port Range (Port-Bereich) die Portnummer ein.

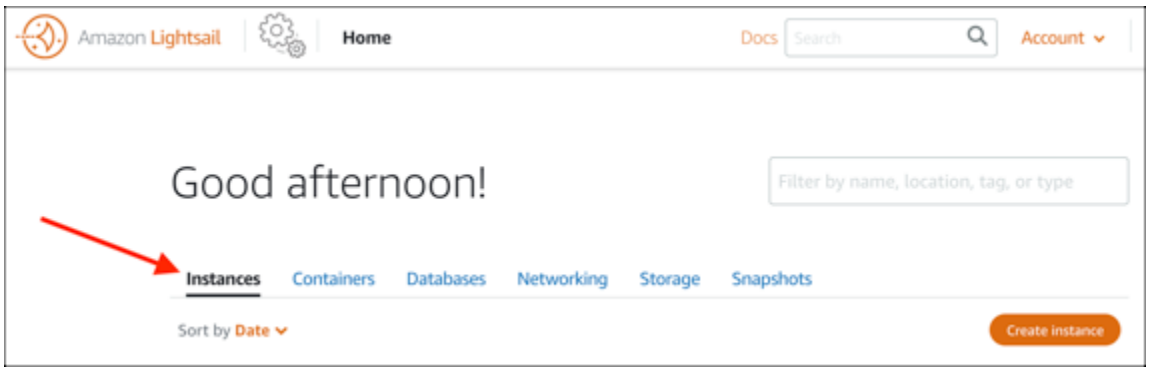
12. Fügen Sie im Textfeld Source (Quelle) die private IP-Adresse Ihrer WordPress-Instance hinzu. Sie müssen die IP-Adressen in CIDR-Notation eingeben, was bedeutet, dass Sie `/32` anhängen müssen. Zum Beispiel, um `192.0.2.0` zuzulassen, geben Sie `192.0.2.0/32` ein.
13. Wählen Sie Save rules (Regeln speichern) aus.



Schritt 3: Herstellen einer Verbindung mit Ihrer Aurora-Datenbank von Ihrer Lightsail-Instance

Schliessen Sie den folgenden Vorgang ab, um zu bestätigen, dass Sie eine Verbindung mit Ihrer Aurora-Datenbank von Ihrer Lightsail-Instance herstellen können.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Instances.

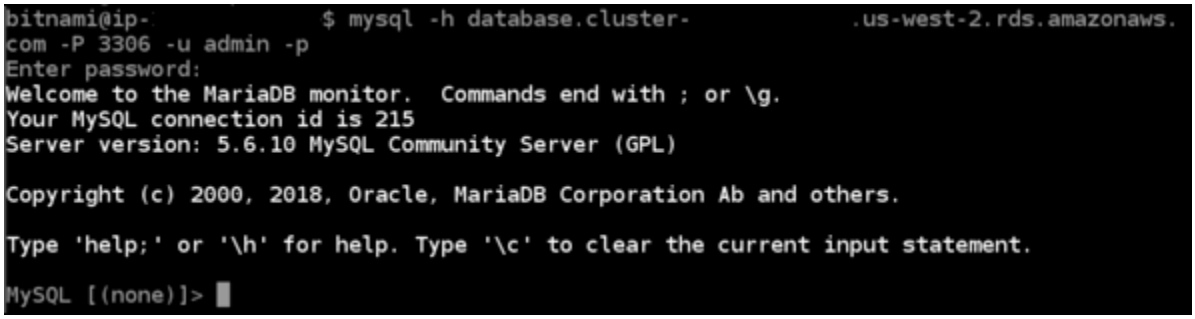


3. Wählen Sie das browserbasierte SSH-Client-Symbol für Ihre WordPress-Instance aus, um mit SSH eine Verbindung herzustellen.

4. Nachdem Sie mit Ihrer Instance verbunden sind, geben Sie den folgenden Befehl ein, um sich mit Ihrer Aurora-Datenbank zu verbinden. Ersetzen Sie *DatabaseEndpoint* durch die Endpunktadresse Ihrer Aurora-Datenbank und ersetzen Sie *Port* durch den Port Ihrer Datenbank. Ersetzen Sie *MyUserName* durch den Namen des Benutzers, den Sie beim Erstellen der Datenbank eingegeben haben.

```
mysql -h DatabaseEndpoint -P Port -u MyUserName -p
```

Sie sollten eine Antwort ähnlich der folgenden sehen, die bestätigt, dass Ihre Instance auf Ihre Aurora-Datenbank zugreifen und eine Verbindung mit dieser herstellen kann.



Wenn Sie diese Antwort nicht sehen oder eine Fehlermeldung angezeigt wird, müssen Sie möglicherweise die Sicherheitsgruppe Ihrer Aurora-Datenbank so konfigurieren, dass die private IP-Adresse Ihrer Lightsail-Instance zulässig ist, um damit eine Verbindung herzustellen. Weitere Informationen finden Sie im Abschnitt Konfigurieren der Sicherheitsgruppe für Ihre Aurora-Datenbank dieses Handbuchs.

Schritt 4: Übertragen der Datenbank von einer WordPress-Instance in Ihre Aurora-Datenbank

Nachdem Sie nun bestätigt haben, dass Sie von Ihrer Instance aus eine Verbindung zu Ihrer Datenbank herstellen können, sollten Sie die Daten von Ihrer WordPress-Datenbank zu Ihrer Aurora-Datenbank übertragen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Registerkarte Instances (Instances) das Symbol für einen browserbasierte SSH-Client für Ihre WordPress-Instance aus.

3. Nachdem der browserbasierte SSH-Client mit Ihrer WordPress-Instance verbunden ist, geben Sie den folgenden Befehl ein. Der Befehl überträgt die Daten aus der `bitnami_wordpress`-Datenbank, die sich auf Ihrer Instance befindet, und verschiebt sie in Ihre Aurora-Datenbank. Ersetzen Sie im Befehl *`DatabaseUserName`* durch den Namen des Hauptbenutzers, den Sie beim Erstellen der Aurora-Datenbank eingegeben haben. Ersetzen Sie *`DatabaseEndpoint`* durch die Endpunktadresse Ihrer Aurora-Datenbank.

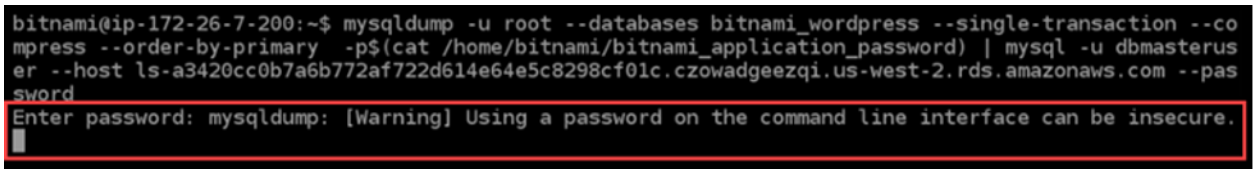
```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password) |
 sudo mysql -u DatabaseUserName --host  DatabaseEndpoint --password
```

   Beispiel

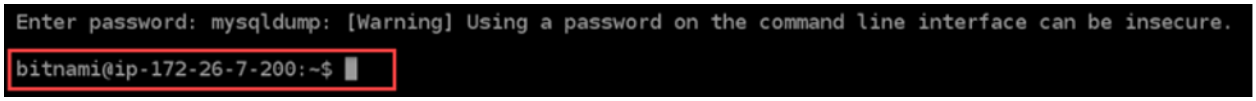
```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password)
 | sudo mysql -u DBuser --host  abc123exampleE67890.czowadgeezqi.us-
west-2.rds.amazonaws.com --password
```

4. Wenn Sie durch `Enter password` dazu aufgefordert werden, geben Sie das Passwort für Ihre Aurora-Datenbank ein und betätigen Sie die Eingabetaste.

Sie können das Passwort während der Eingabe nicht sehen.



Eine Antwort ähnlich dem folgenden Beispiel wird bei erfolgreicher Übertragung der Daten angezeigt:



Wenn Sie eine Fehlermeldung erhalten, stellen Sie zunächst sicher, dass Datenbank-Benutzername, Passwort und Endpunkt korrekt sind, und versuchen Sie es erneut.

Schritt 5: Konfigurieren von WordPress, um eine Verbindung zu Ihrer Aurora-Datenbank herzustellen

Nachdem Sie Ihre Anwendungsdaten an Ihre Aurora-Datenbank übertragen haben, sollten Sie WordPress so konfigurieren, dass es eine Verbindung dahin herstellt. Führen Sie die folgenden Schritte aus, um die WordPress-Konfigurationsdatei (`wp-config.php`) so zu bearbeiten, dass Ihre Website eine Verbindung zu Ihrer Aurora-Datenbank herstellt.

1. Geben Sie im browserbasierten SSH-Client, der mit Ihrer WordPress-Instance verbunden ist, den folgenden Befehl ein, um ein Backup der `wp-config.php`-Datei zu erstellen.

   ```
   cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-config.php-backup
   ```

2. Geben Sie den folgenden Befehl ein, um die `wp-config.php`-Datei schreibfähig zu machen:

   ```
   sudo chmod 664 /opt/bitnami/wordpress/wp-config.php
   ```

3. Ersetzen Sie den Datenbankbenutzernamen in der `config`-Datei durch den Namen des Hauptbenutzers, den Sie beim Erstellen der Aurora-Datenbank eingegeben haben.

   ```
   sudo wp config set DB_USER DatabaseUserName
   ```

4. Ersetzen Sie den Datenbank-Host in der `config`-Datei durch die Endpunktadresse und Portnummer Ihrer Aurora-Datenbank. Zum Beispiel `abc123exampleE67890.czowadgeezqi.us-west-2.rds.amazonaws.com:3306`.

   ```
   sudo wp config set DB_HOST DatabaseEndpoint:Port
   ```

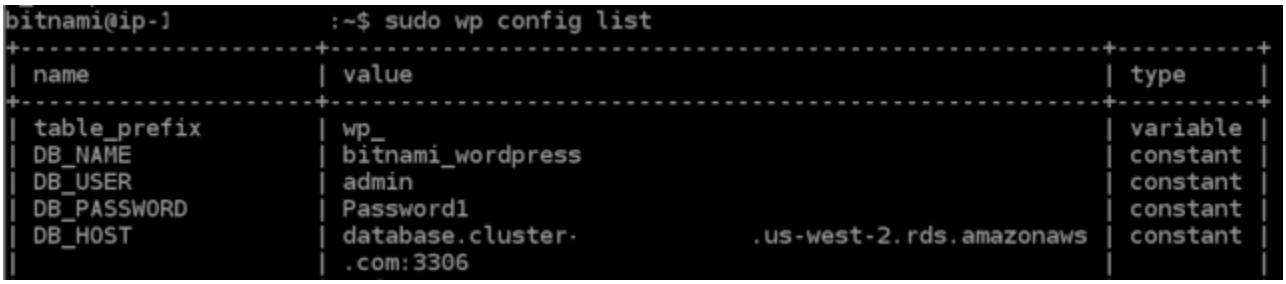
5. Ersetzen Sie das Datenbankpasswort in der `config`-Datei durch das Passwort für Ihre Aurora-Datenbank.

   ```
   sudo wp config set DB_PASSWORD DatabasePassword
   ```

6. Geben Sie den `wp config list`-Befehl ein, um zu überprüfen, ob die Informationen, die Sie in der `wp-config.php`-Datei eingegeben haben, richtig sind.

   ```
   sudo wp config list
   ```

   Es wird ein Ergebnis ähnlich dem folgenden angezeigt, das Ihre Konfigurationsdetails anzeigt:

7. Geben Sie den folgenden Befehl ein, um die Webservices auf Ihrer Instance neu zu starten.

   ```
   sudo /opt/bitnami/ctlscript.sh restart
   ```

   Nach dem Neustart der Services wird ein Ergebnis ähnlich dem folgenden angezeigt:

   Herzlichen Glückwunsch! Ihre WordPress-Website ist jetzt so konfiguriert, dass sie Ihre Aurora-Datenbank verwendet.

> **Note**
>
> Wenn Sie die ursprüngliche `wp-config.php`-Datei wiederherstellen müssen, geben Sie den folgenden Befehl ein, um sie unter Verwendung des Backups wiederherzustellen, das Sie zuvor in diesem Tutorial erstellt haben:
>
> ```
> cp /opt/bitnami/wordpress/wp-config.php-backup /opt/bitnami/wordpress/wp-config.php
> ```

Tutorial: Verbinden Ihrer WordPress-Website mit einer MySQL-verwalteten Datenbank in Lightsail

Wichtige WordPress-Website-Daten für Beiträge, Seiten und Benutzer werden in der MySQL-Datenbank gespeichert, die auf der Instance in Amazon Lightsail ausgeführt wird. Wenn die WordPress-Instance ausfällt, können Sie Ihre Daten möglicherweise nicht wiederherstellten. Um dieses Szenario zu vermeiden, sollten Sie Ihre Websitedaten in eine MySQL-verwaltete Datenbank in übertragen.

In diesem Tutorial erfahren Sie, wie Sie Ihre WordPress-Websitedaten für Beiträge, Seiten und Benutzer in eine MySQL-verwaltete Datenbank in Lightsail übertragen. Außerdem wird gezeigt, wie Sie die WordPress-Konfigurationsdatei (`wp-config.php`) so bearbeiten, dass sich Ihre WordPress-Website mit der neuen verwalteten Datenbank verbindet und nicht mehr die auf der Instance ausgeführte Datenbank verwendet.

Inhalt

Schritt 1: Erfüllen der Voraussetzungen

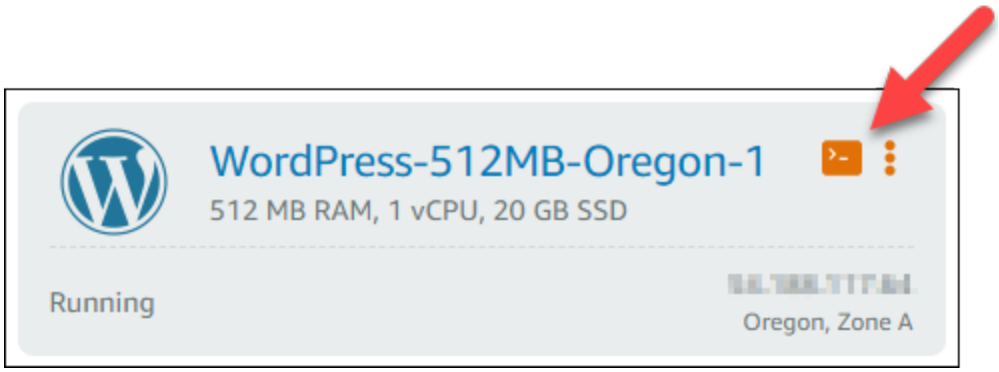
Erfüllen Sie die folgenden Voraussetzungen, bevor Sie beginnen:

- Erstellen Sie eine WordPress-Instance inLightsail und stellen Sie sicher, dass sie ausgeführt wird. Weitere Informationen finden Sie im Tutorial: Starten und Konfigurieren einer WordPress-Instance in Amazon Lightsail.
- Erstellen Sie eine MySQL-verwaltete Datenbank in Lightsail in derselben AWS-Region wie Ihre WordPress-Instance und stellen Sie sicher, dass sie ausgeführt wird. WordPress funktioniert mit allen in Lightsail verfügbaren MySQL-Datenbankoptionen . Weitere Informationen finden Sie unter Erstellen einer Datenbank in Amazon Lightsail.
- Aktivieren Sie den öffentlichen und den Datenimportmodus für Ihre MySQL-verwaltete Datenbank. Sie können diese Modi deaktivieren, nachdem Sie die Schritte in diesem Tutorial durchgeführt haben. Weitere Informationen finden Sie unter Konfigurieren des öffentlichen Modus für Ihre Datenbank und Konfigurieren des Datenimportmodus für Ihre Datenbank.

Schritt 2: Übertragen der WordPress-Datenbank in eine MySQL-verwaltete Datenbank in

Führen Sie die folgenden Schritte aus, um die Übertragung Ihrer WordPress-Websitedaten in Ihre MySQL-verwaltete Datenbank in durchzuführen.Lightsailaus.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Registerkarte Instances das browserbasierte SSH-Client-Symbol für Ihre WordPress-Instance aus.



3. Nachdem der browserbasierte SSH-Client mit Ihrer WordPress-Instance verbunden ist, geben Sie den folgenden Befehl ein, um die `bitnami_wordpress`-Datenbank auf der Instance zu Ihrer MySQL-verwalteten Datenbank zu übertragen. Stellen Sie sicher, dass Sie *`DbUserName`* durch den Benutzernamen für Ihre verwaltete Datenbank ersetzen, und ersetzen Sie *`DbEndpoint`* durch die Endpunktadresse für Ihre verwaltete Datenbank.

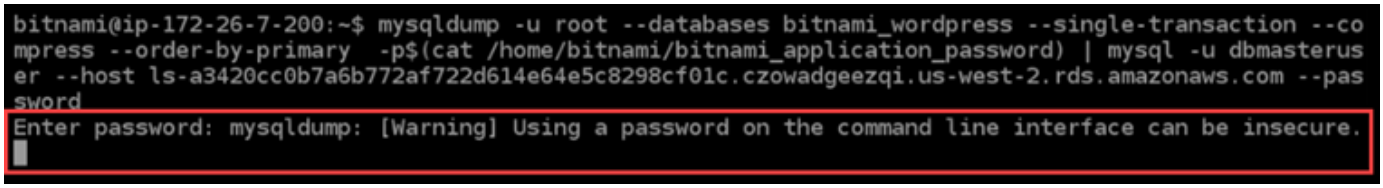
```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary  -p$(cat /home/bitnami/bitnami_application_password) |
 sudo mysql -u DbUserName --host DbEndpoint --password
```

Beispiel

```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password)
 | sudo mysql -u dbmasteruser --host ls-abc123exampleE67890.czowadgeezqi.us-
west-2.rds.amazonaws.com --password
```

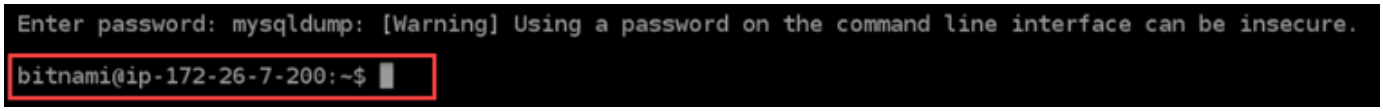
4. Wenn Sie dazu aufgefordert werden, geben Sie das Passwort für Ihre MySQL-verwaltete Datenbank ein und betätigen Sie die Eingabetaste.

   Sie sehen das Passwort während der Eingabe nicht.



5. Ein Ergebnis ähnlich dem folgenden Beispiel wird bei erfolgreicher Übertragung der Daten angezeigt.

   Wenn Sie eine Fehlermeldung erhalten, stellen Sie zunächst sicher, dass Datenbank-Benutzername, Passwort und Endpunkt korrekt sind, und versuchen Sie es erneut.



Schritt 3: Konfigurieren von WordPress, um eine Verbindung zu Ihrer MySQL-verwalteten Datenbank herzustellen

Führen Sie die folgenden Schritte aus, um die WordPress-Konfigurationsdatei (`wp-config.php`) so zu bearbeiten, dass Ihre Website eine Verbindung zu Ihrer MySQL-verwalteten Datenbank herstellt.

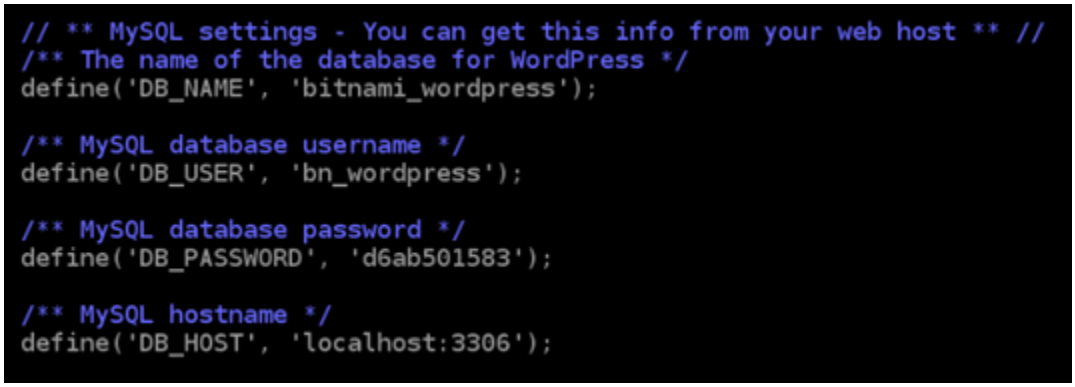
1. Geben Sie im browserbasierten SSH-Client, der mit Ihrer WordPress-Instance verbunden ist, den folgenden Befehl ein, um ein Backup der WordPress-Konfigurationsdatei `wp-config.php` für den Fall eines Fehlers erstellt.

```
cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-config.php-backup
```

2. Geben Sie den folgenden Befehl ein, um die Datei mit `wp-config.php`, einem Texteditor, zu öffnen.

```
nano /opt/bitnami/wordpress/wp-config.php
```

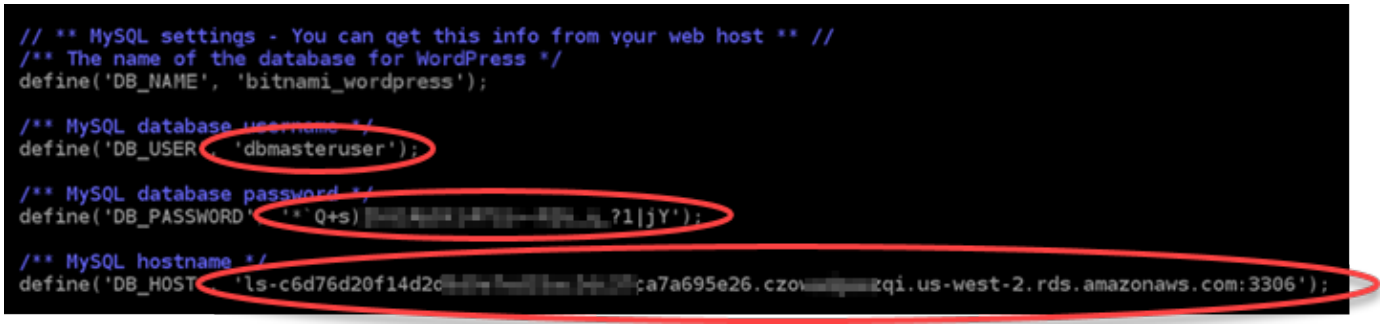
3. Scrollen Sie nach unten, bis Sie die Werte für `DB_USER`, `DB_PASSWORD`, und `DB_HOST` finden, wie esim folgenden Beispiel gezeigt wird.



4. Ändern Sie die folgenden Werte:

   - DB_USER – Bearbeiten Sie dies entsprechend dem Master-Benutzernamen für die MySQL-verwaltete Datenbank. Der Standard-Master-Benutzername für Lightsailverwaltete Datenbanken ist`dbmasteruser` .
   - DB_PASSWORD – Bearbeiten Sie dies entsprechend dem Kennwort für die MySQL-verwaltete Datenbank. Weitere Informationen finden Sie unter Verwaltung Ihres Datenbankpassworts.
   - DB_HOST – Bearbeiten Sie dies entsprechend dem Endpunkt für die MySQL-verwaltete Datenbank. Stellen Sie sicher, dass die `:3306`-Port-Nummer am Ende der Host-Adresse hinzugefügt wird. Zum Beispiel `ls-abc123exampleE67890.czowadgeezqi.us-west-2.rds.amazonaws.com:3306`.

   Das Ergebnis sollte wie folgt aussehen:



5. Betätigen Sie Strg+X, um Nano zu verlassen, und dann Y und die Eingabetaste, um Ihre Änderungen an der WordPress-Konfigurationsdatei zu speichern.
6. Geben Sie den folgenden Befehl ein, um den Apache-Dienst auf Ihrer Instance neu zu starten.

```
sudo /opt/bitnami/ctlscript.sh restart
```

Nach dem Neustart der Servcies wird ein Ergebnis wie das folgende angezeigt:

Herzlichen Glückwunsch! Ihre WordPress-Website ist jetzt so konfiguriert, dass sie die MySQL-verwaltete Datenbank verwendet.

> **Note**
>
> Wenn Sie aus irgendeinem Grund die ursprüngliche `wp-config.php`-Datei wiederherstellen müssen, geben Sie den folgenden Befehl ein, um sie unter Verwendung des Backups wiederherzustellen, die Sie zuvor in diesem Tutorial erstellt haben:
>
> ```
> cp /opt/bitnami/wordpress/wp-config.php-backup /opt/bitnami/wordpress/wp-config.php
> ```

Schritt 4: Abschluss der nächsten Schritte

Führen Sie die folgenden Schritte aus, nachdem Sie eine Verbindung Ihrer WordPress-Website mit einer MySQL-verwalteten Datenbank hergestellt haben.

- Erstellen Sie einen Snapshot Ihrer WordPress-Instance. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Linux- oder Unix-Instance.
- Sie sollten auch einen Snapshot der MySQL-verwalteten Datenbank erstellen. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Datenbank.
- Deaktivieren Sie den öffentlichen und den Datenimportmodus für die MySQL-verwaltete Datenbank. Weitere Informationen finden Sie unter Konfigurieren des öffentlichen Modus für Ihre Datenbank und Konfigurieren des Datenimportmodus für Ihre Datenbank.

Tutorial: Verbinden einer WordPress Instance mit einem Lightsail-Bucket

In diesem Tutorial werden die Schritte beschrieben, die erforderlich sind, um Ihre WordPress Website, die auf einer Amazon Lightsail-Instance ausgeführt wird, mit einem Lightsail-Bucket zu verbinden. Sie können den Bucket verwenden, um statische Inhalte wie Bilder und Anlagen zu hosten. Dazu müssen Sie das WP Offload Media Lite-Plugin auf Ihrer WordPress Website installieren und es für die Verbindung mit Ihrem Lightsail-Bucket konfigurieren. Nachdem das Plugin konfiguriert wurde, werden alle Medien, die Sie auf Ihre WordPress Website hochladen, automatisch zu Ihrem Bucket anstelle der Festplatte der Instance hinzugefügt.

Inhalt

Schritt 1: Erfüllen der Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies noch nicht geschehen ist:

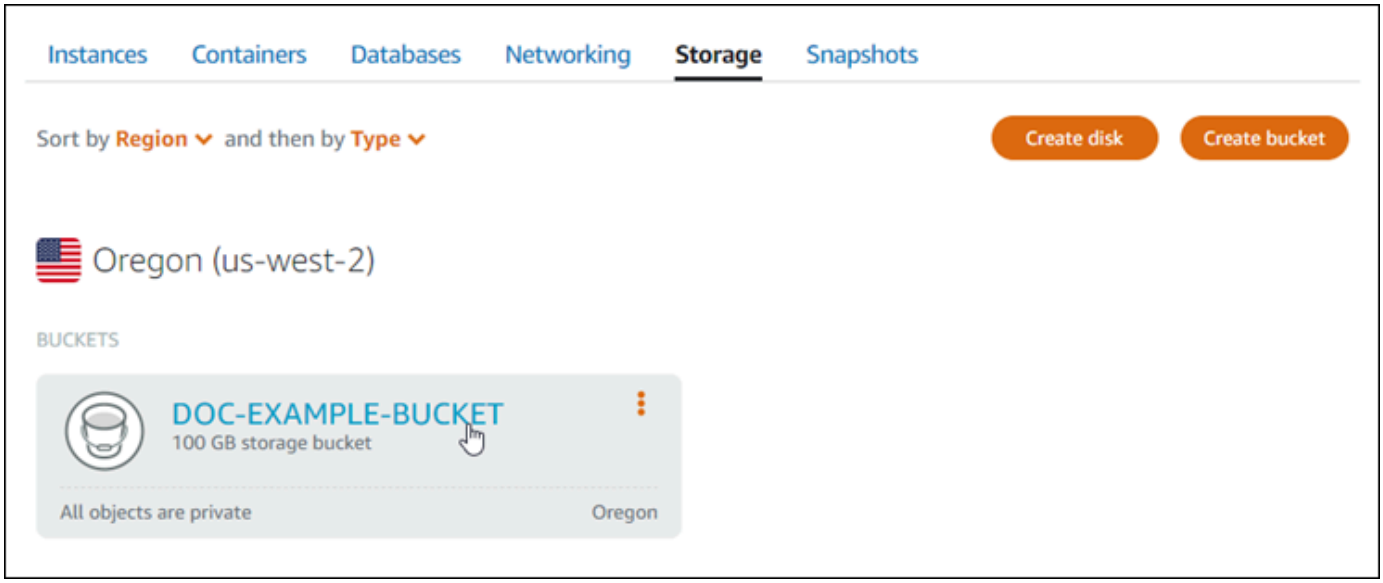
- Erstellen Sie eine WordPress Instance in Lightsail. Weitere Informationen finden Sie unter Tutorial: Starten und Konfigurieren einer WordPress Instance in Amazon Lightsail.

- Erstellen Sie einen Bucket im Lightsail-Objektspeicherdienst. Weitere Informationen finden Sie unter Einen Bucket erstellen.

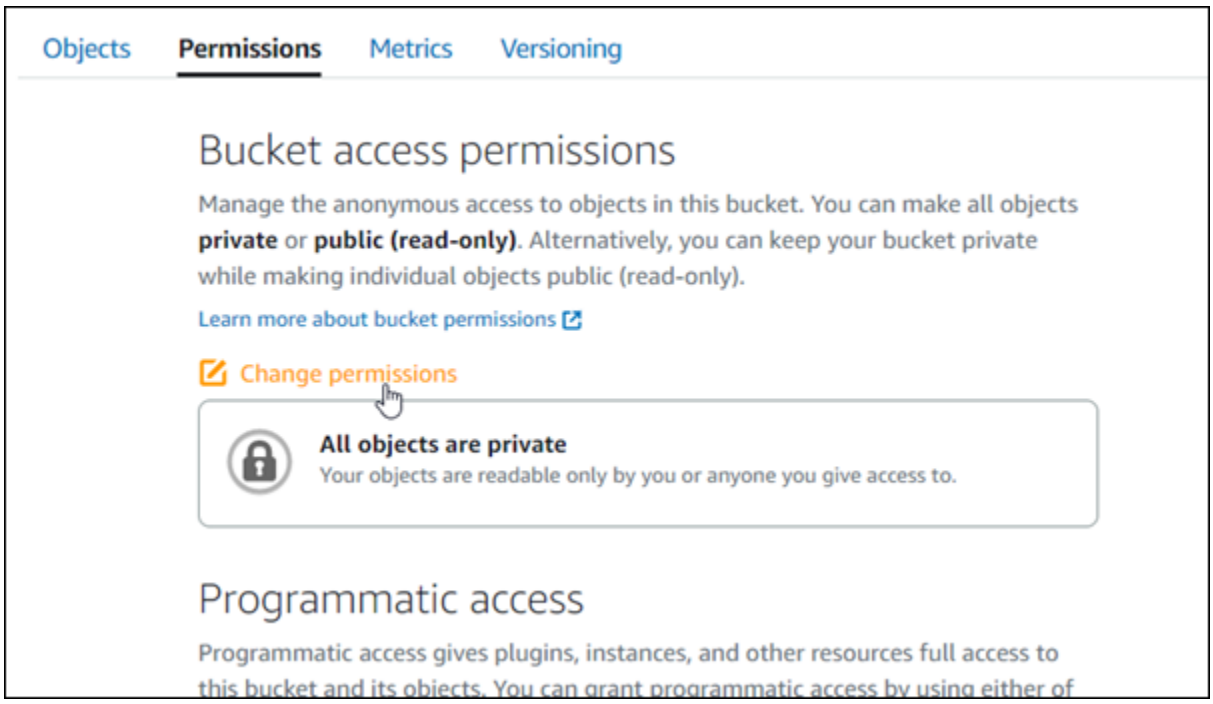
Schritt 2: Ändern der Bucket-Berechtigungen

Führen Sie das folgende Verfahren aus, um die Berechtigungen Ihres Buckets zu ändern, um Zugriff auf Ihre WordPress Instance und das Offload Media Lite-Plugin zu gewähren. Die Zugriffsberechtigungen Ihres Buckets müssen auf Einzelne Objekte können öffentlich gemacht werden (schreibgeschützt) aus. Sie müssen die WordPress Instance auch an die Zugriffsrolle Ihres Buckets anfügen. Weitere Informationen zu Bucket-Berechtigungen finden Sie unter Bucket-Berechtigungen.

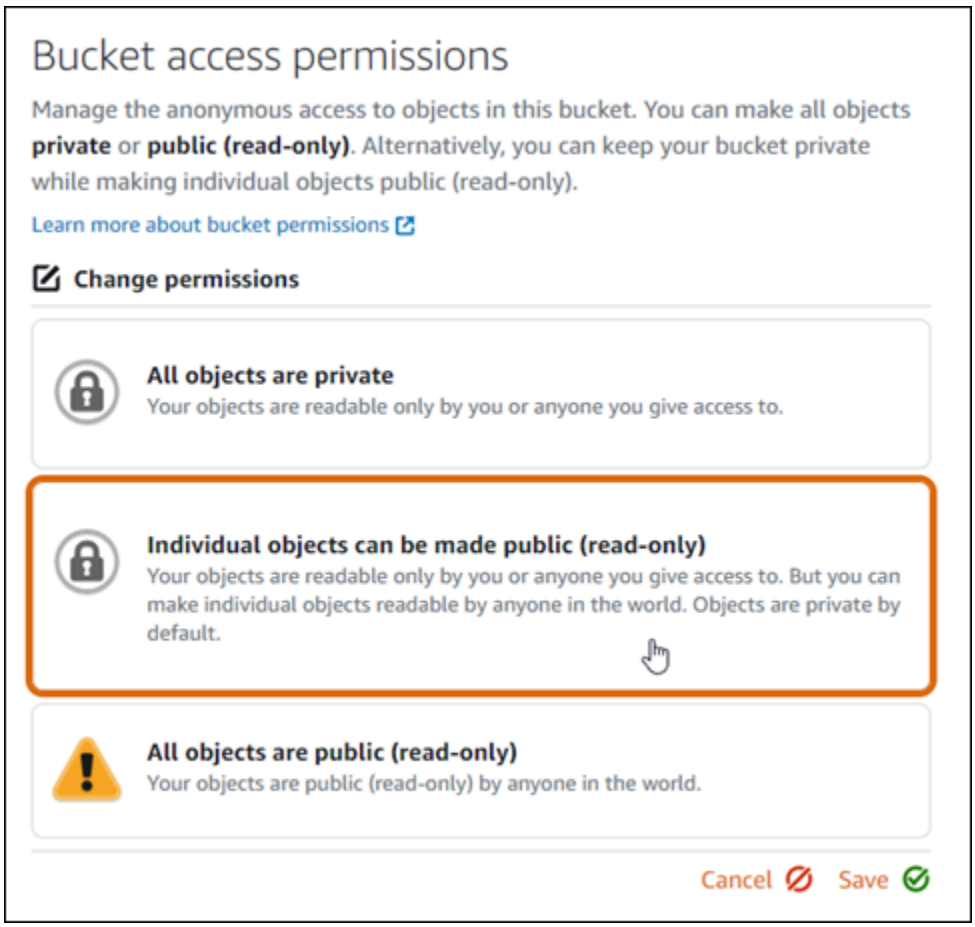
1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Speicher aus.
3. Wählen Sie den Namen des Buckets aus, den Sie mit Ihrer WordPress Website verwenden möchten.



4. Wählen Sie die Registerkarte Berechtigungen auf der Seite Bucket-Verwaltung aus.
5. Wählen Sie Ändern von Berechtigungen unter Abschnitt Zugriffsberechtigungen für Buckets der Seite.

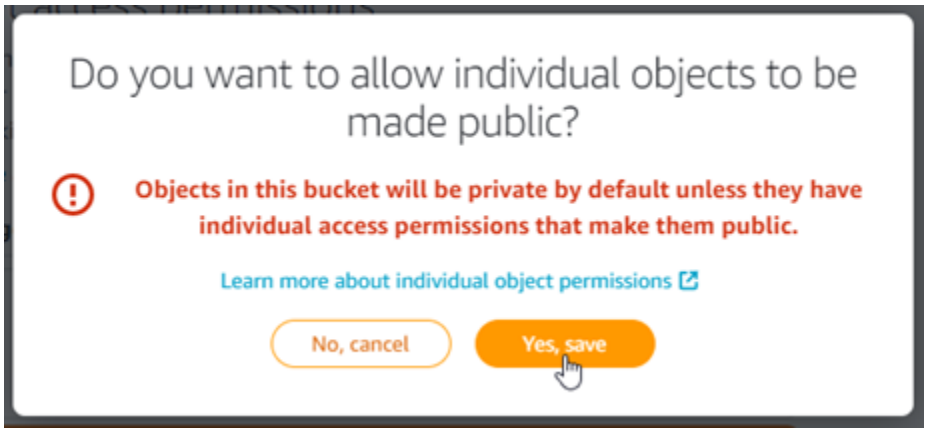


6. Wählen Sie Einzelne Objekte können öffentlich und schreibgeschützt gemacht werden.



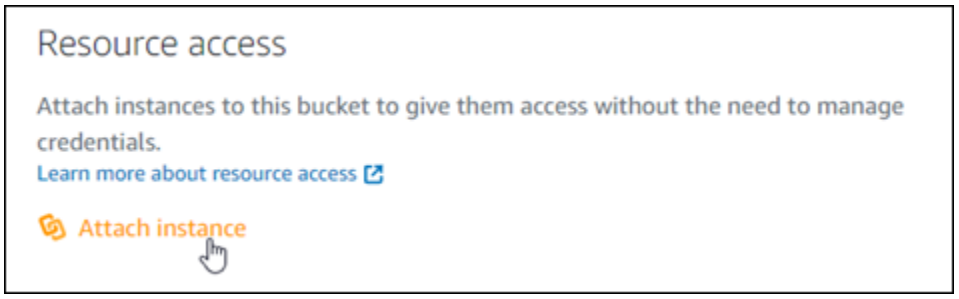
7. Wählen Sie Speichern.

8. Wählen Sie in der angezeigten Bestätigungsaufforderung Ja, speichern.

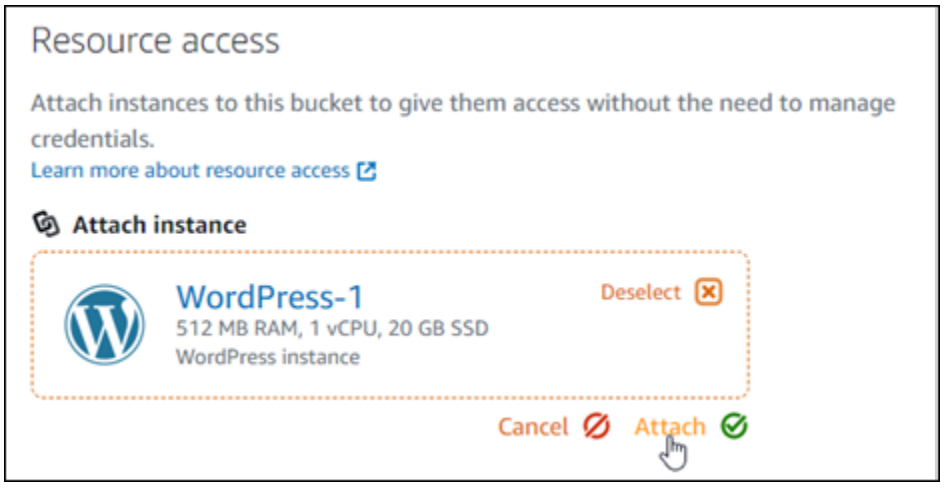


Nach einigen Augenblicken ist Ihr Bucket so konfiguriert, dass ein individueller Objektzugriff möglich ist. Dadurch wird sichergestellt, dass Objekte, die von Ihrer WordPress Website mit dem Offload Media Lite-Plugin in Ihren Bucket hochgeladen werden, für Ihre Kunden lesbar sind.

9. Scrollen Sie zum Abschnitt Zugriff auf Ressourcen der Seite und wählen Sie Instance hinzufügen.



10. Wählen Sie den Namen Ihrer WordPress Instance in der daraufhin angezeigten Dropdown-Liste aus und klicken Sie dann auf Attach .



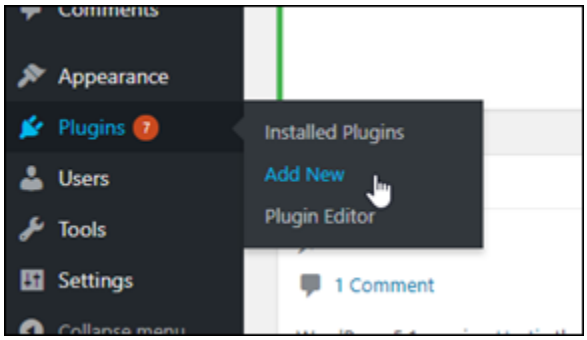
Nach einigen Augenblicken ist Ihre WordPress Instance mit Ihrem Bucket verbunden. Dadurch erhält Ihre WordPress Instance Zugriff auf die Verwaltung Ihres Buckets und seiner Objekte.

Schritt 3: Installieren des WP-Offload-Media-Lite-Plugins auf Ihrer WordPress Website

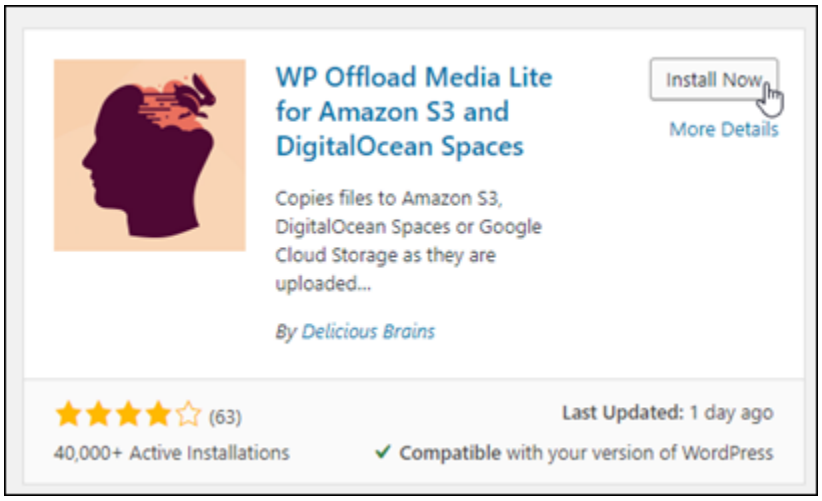
Führen Sie das folgende Verfahren aus, um das WP Offload Media Lite-Plugin auf Ihrer WordPress Website zu installieren. Dieses Plugin kopiert automatisch Bilder, Videos, Dokumente und andere Medien, die über den WordPress Medien-Uploader hinzugefügt wurden, in Ihren Lightsail-Bucket. Weitere Informationen finden Sie unter WP Offload Media Lite auf der WordPress Website .

1. Melden Sie sich beim Dashboard Ihrer WordPress Website als Administrator an.

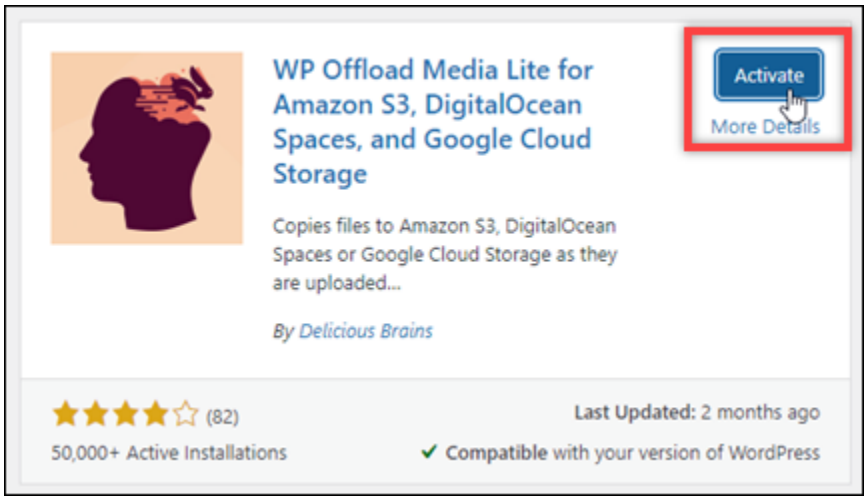
   Weitere Informationen finden Sie unter Abrufen des Anwendungsbenutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.
2. Pausieren Sie Plugins im linken Navigationsmenü und wählen Sie Add New (Neues auswählen).



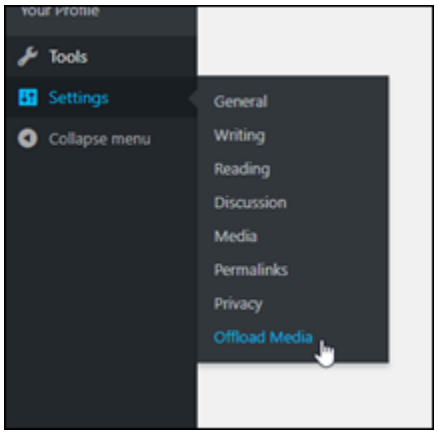
3. Suchen Sie nach WP Offload Media Lite.
4. Wählen Sie in den Suchergebnissen Install Now (Jetzt installieren) neben dem WP Offload Media-Plug-In aus.



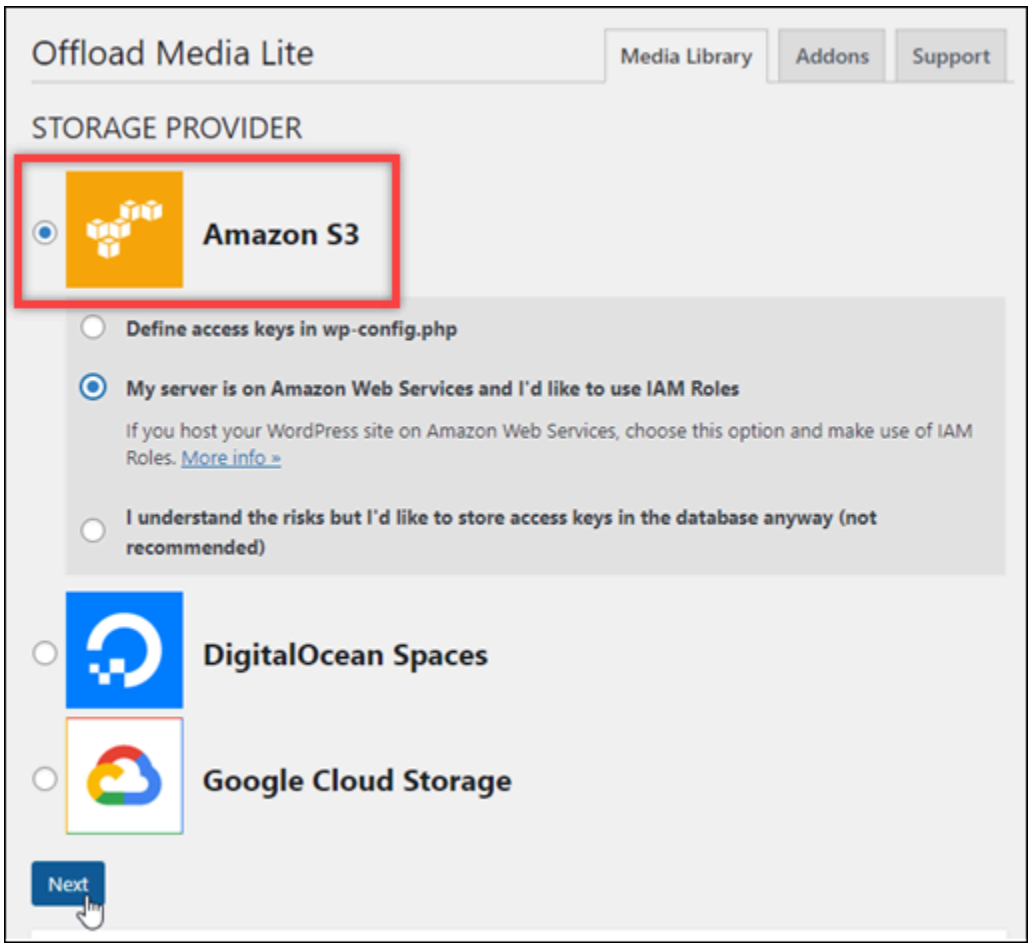
5. Wählen Sie Activate (Aktivieren) aus, nachdem das Plug-In installiert wurde.



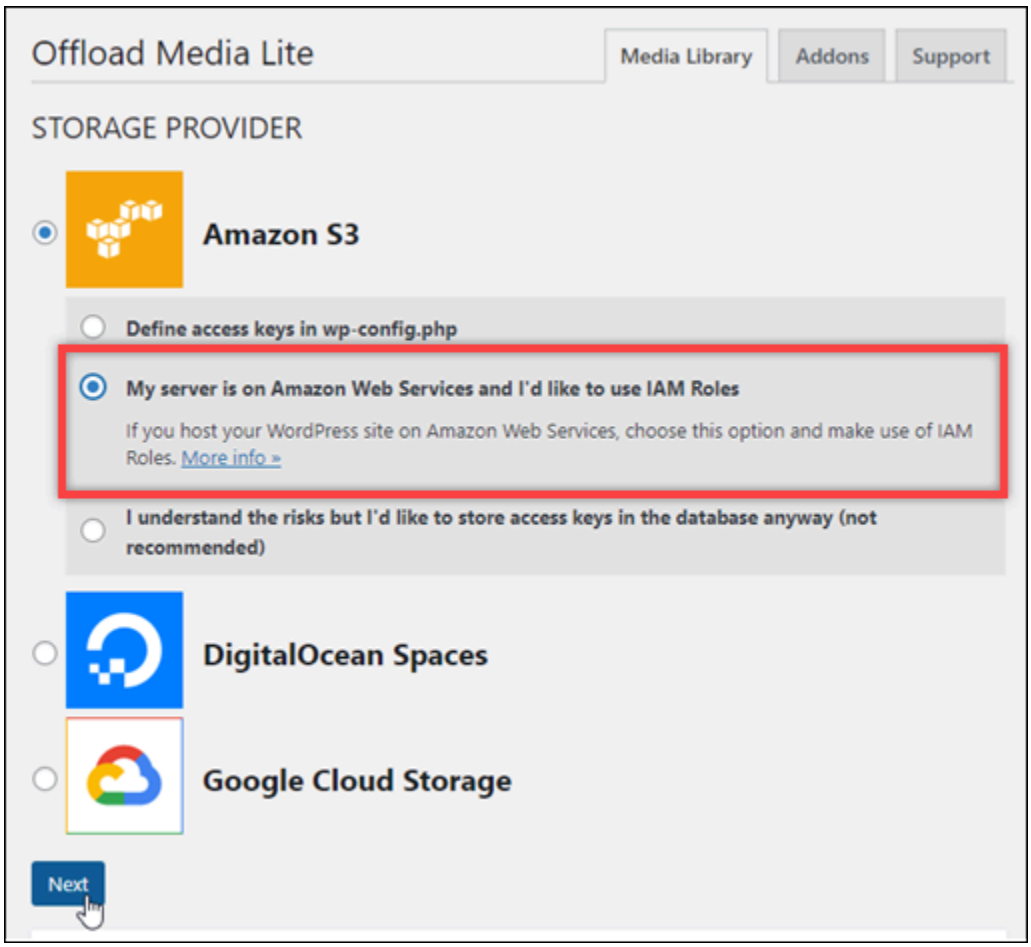
6. Wählen Sie im linken Navigationsmenü Settings (Einstellungen) und dann Offload Media (Medien auslagern) aus.



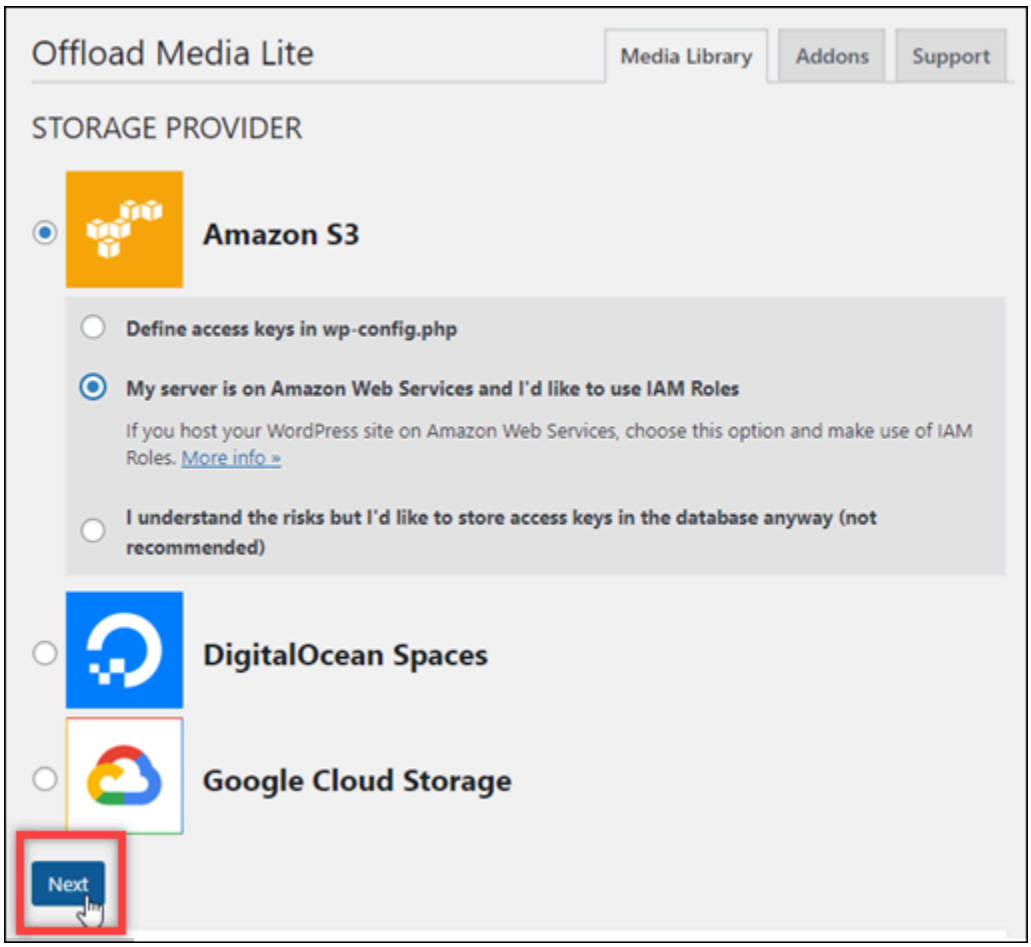
7. In der Offload Medien-Seite, wählen Sie Amazon S3 als Speicheranbieter.



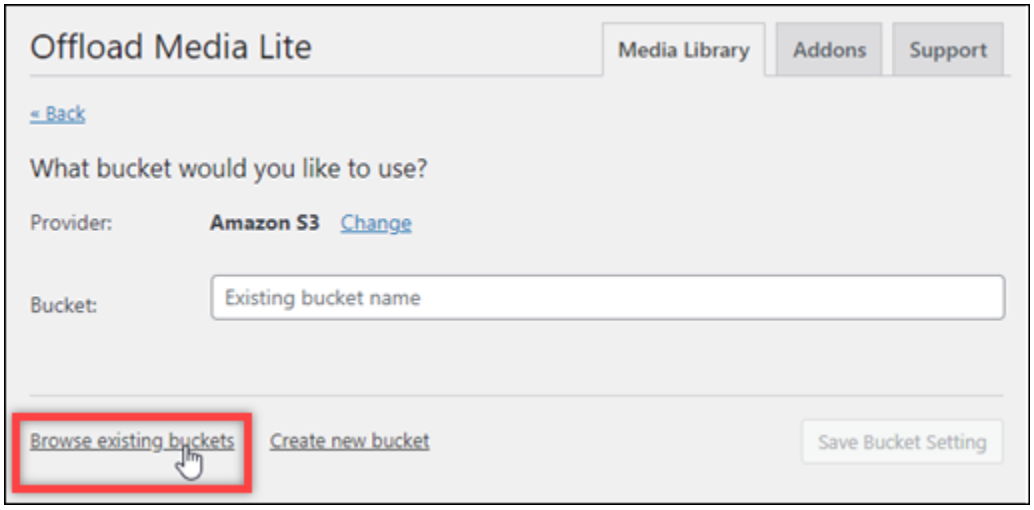
8. Klicken Sie auf Mein Server ist auf Amazon Web Services und ich möchte IAM-Rollen verwenden aus.



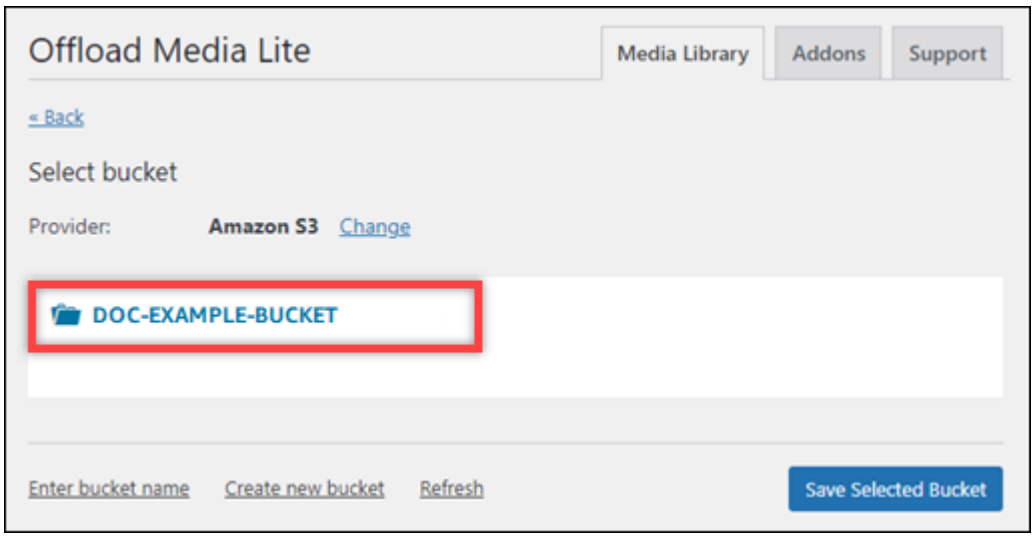
9. Wählen Sie Weiter aus.



10. Klicken Sie auf Durchsuchen vorhandener Buckets auf der Seite Welches Bucket möchten Sie verwenden?, die angezeigt wird.

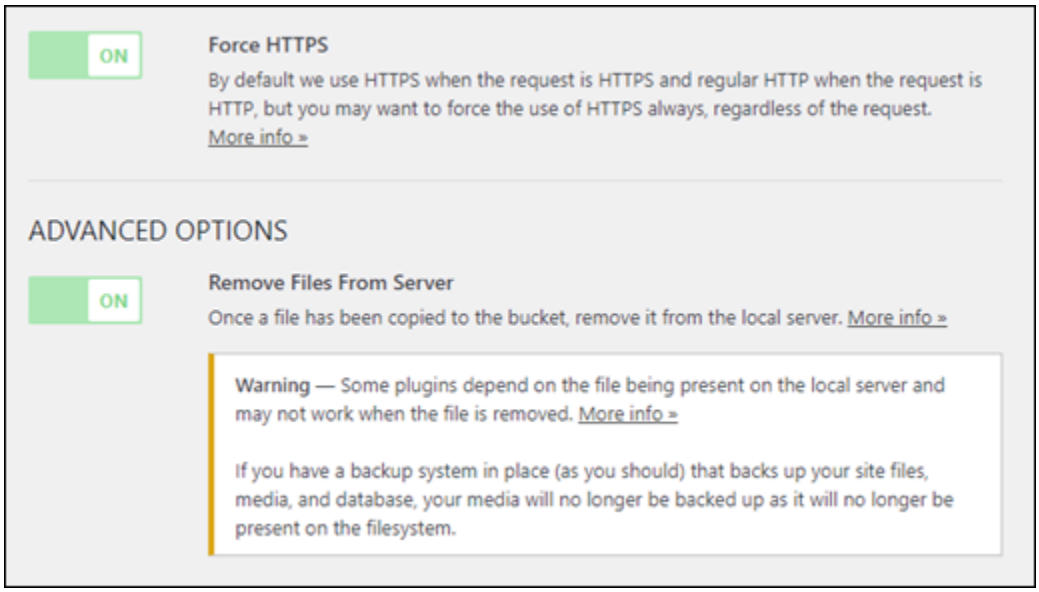


11. Wählen Sie den Namen des Buckets aus, den Sie mit Ihrer WordPress Instance verwenden möchten.



12. In derMedia Lite-Einstellungen auslagern, die angezeigt wird, stellen Sie sicher, dass Erzwingen von HTTPS und Dateien vom Server entfernen aus.

    - Die Einstellung HTTPS erzwingen muss aktiviert sein, da Lightsail-Buckets standardmäßig HTTPS verwenden, um Mediendateien bereitzustellen. Wenn Sie diese Funktion nicht aktivieren, werden Mediendateien, die von Ihrer WordPress Website in Ihren Lightsail-Bucket hochgeladen werden, nicht korrekt an Ihre Website-Besucher bereitgestellt.
    - Die Einstellung Dateien vom Server entfernen stellt sicher, dass Medien, die in Ihren Lightsail-Bucket hochgeladen werden, nicht auch auf der Festplatte Ihrer Instance gespeichert werden. Wenn Sie diese Funktion nicht aktivieren, werden Mediendateien, die in Ihren Lightsail-Bucket hochgeladen werden, auch im lokalen Speicher Ihrer Instance gespeichert WordPress .



13. Wählen Sie Save Changes.

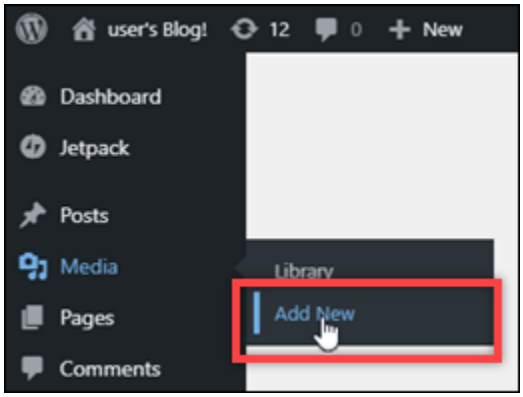
> **Note**
>
> Um später zur Seite Media-Lite-Einstellungen auslagern zurückzukehren, pausieren Sie Einstellungen im linken Navigationsmenü und wählen Sie Media Lite auslagern.

Ihre WordPress Website ist jetzt für die Verwendung des Media-Lite-Plugins konfiguriert. Wenn Sie das nächste Mal eine Mediendatei über hochladen WordPress, wird diese Datei automatisch in Ihren Lightsail-Bucket hochgeladen und vom Bucket bereitgestellt. Fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort, um die Konfiguration zu testen.

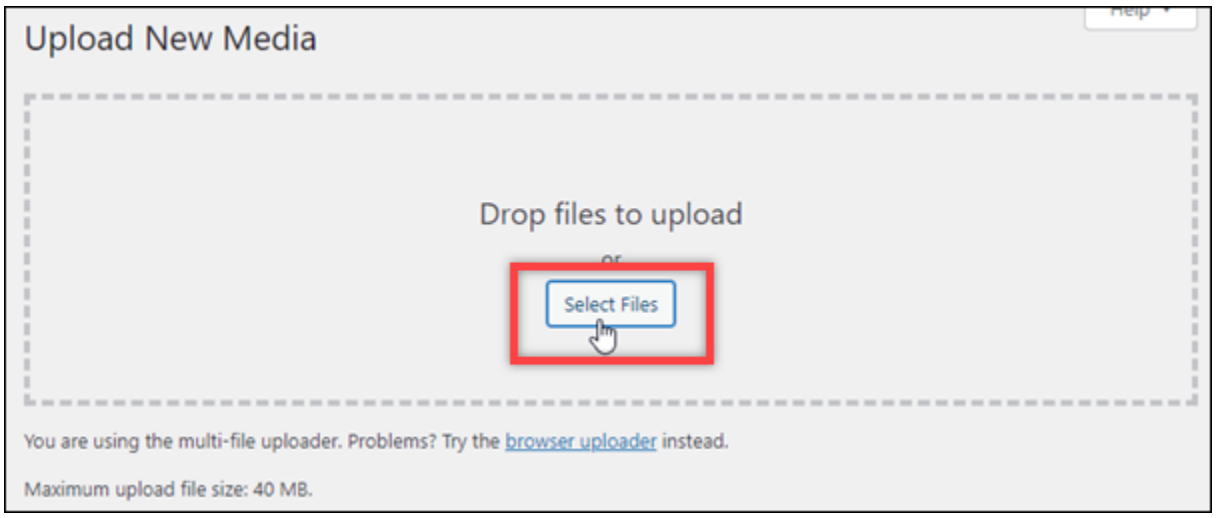
Schritt 4: Testen der Verbindung zwischen Ihrer WordPress Website und Ihrem Lightsail-Bucket

Führen Sie das folgende Verfahren aus, um eine Mediendatei auf Ihre WordPress Instance hochzuladen und zu bestätigen, dass sie in Ihren Lightsail-Bucket hochgeladen und aus diesem bereitgestellt wird.

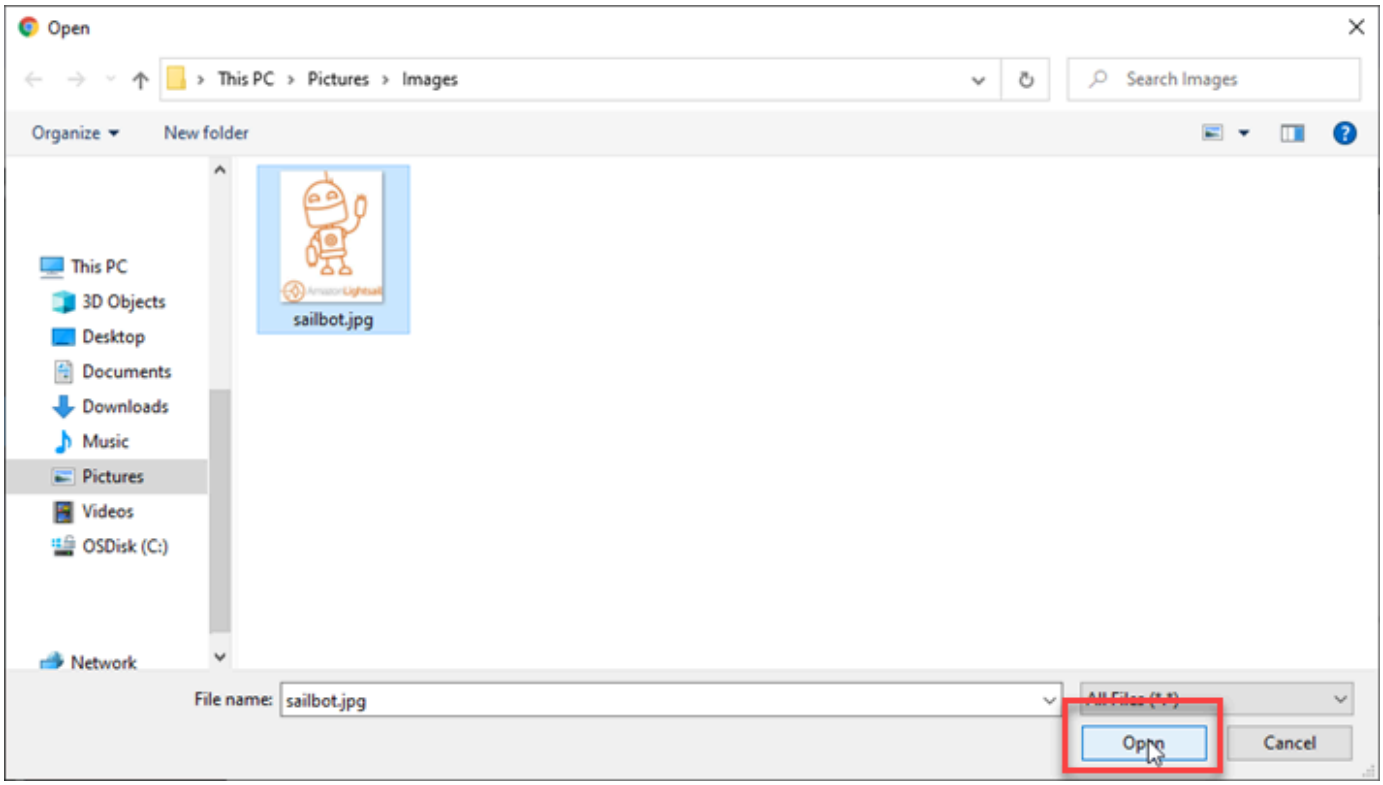
1. Pausieren Sie im linken Navigationsmenü des WordPress Dashboards auf Medien und wählen Sie Neu hinzufügen aus.



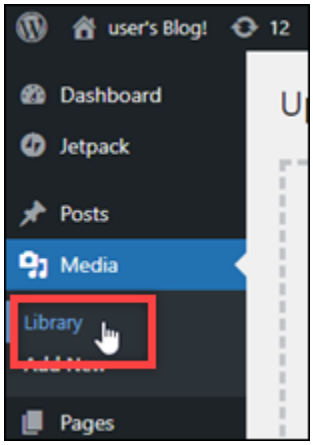
2. Wählen Sie Dateien auswählen auf der Seite Neue Medien uploaden die angezeigt wird.



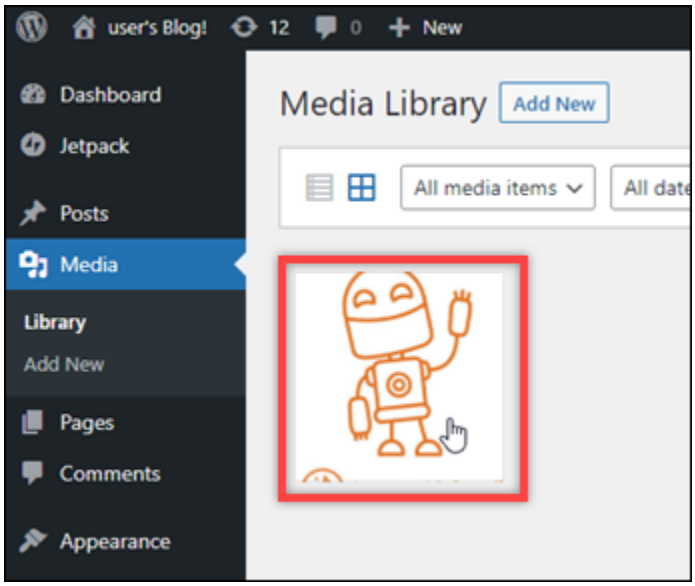
3. Wählen Sie eine Mediendatei aus, die von Ihrem lokalen Computer hochgeladen werden soll, und wählen Sie Öffnen aus.



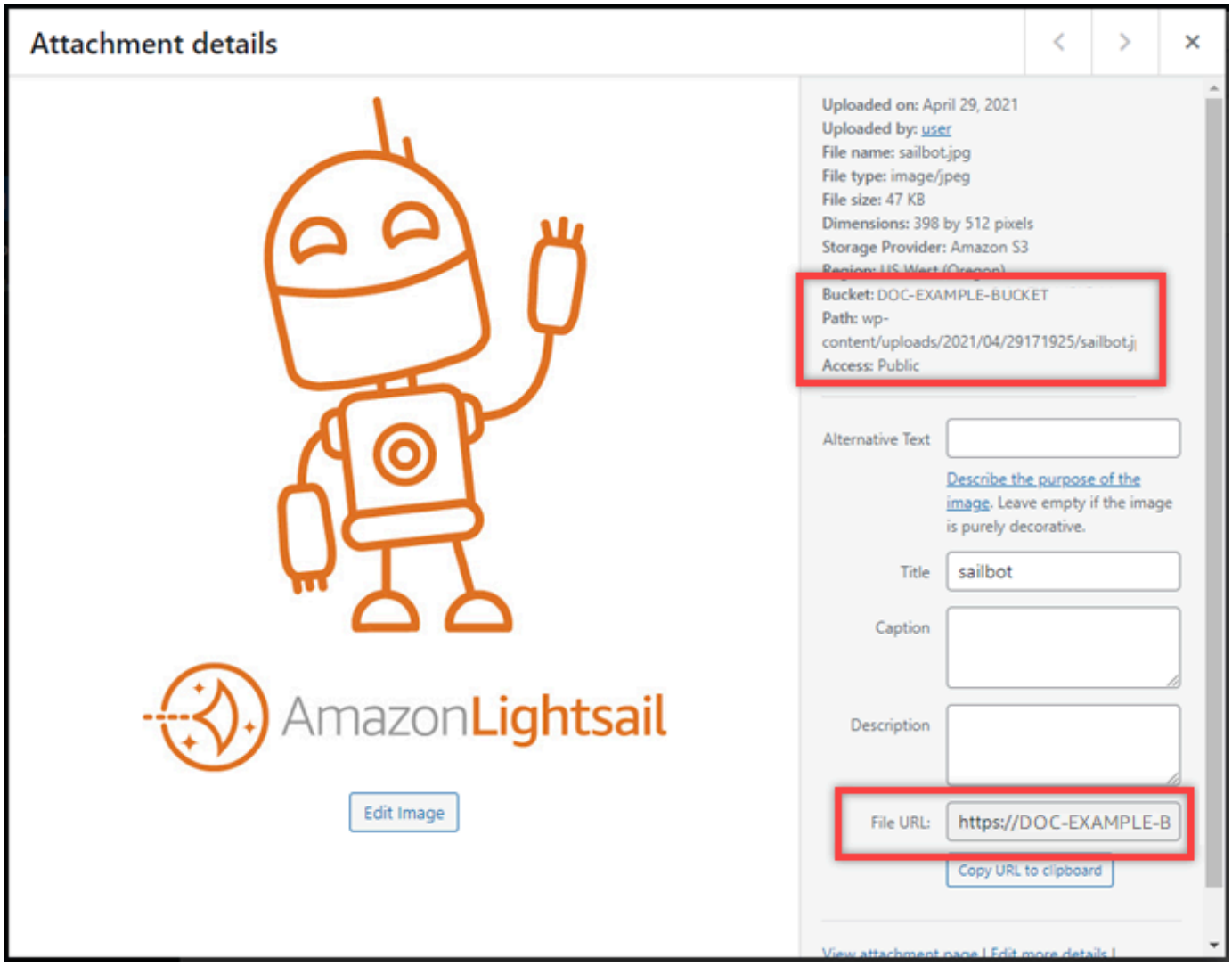
4. Wenn die Datei hochgeladen wurde, wählen Sie Bibliothek unter Medien im linken Navigationsmenü.



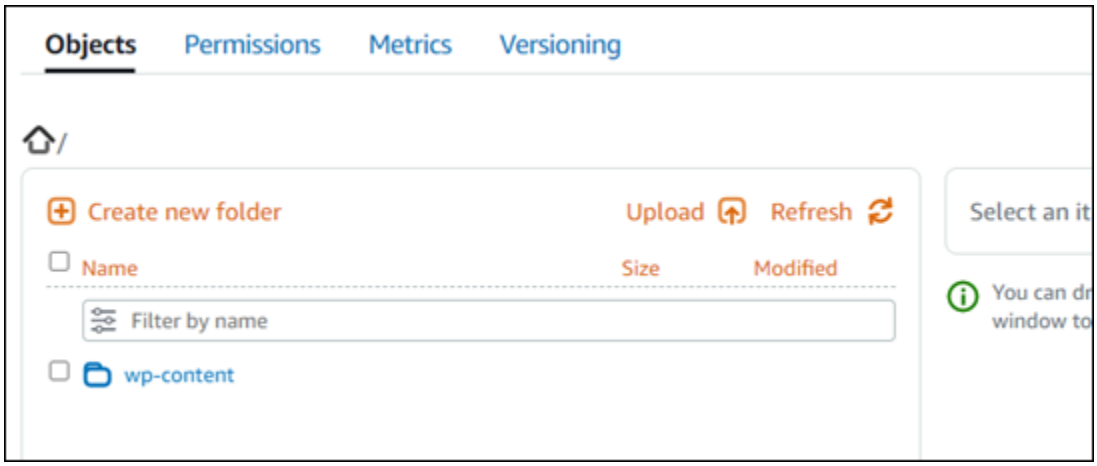
5. Wählen Sie die Datei aus, die Sie kürzlich hochgeladen haben.



6. Im Detailbereich der Datei sollten Sie den Namen Ihres Buckets im Bucket und URL der Datei unterscheiden sich nicht.



7. Wenn Sie auf der Lightsail-Bucket-Verwaltungsseite zur Registerkarte Objekte wechseln, sollten Sie einen wp-content-Ordner sehen. Dieser Ordner wird durch das Offload-Media Lite-Plug-In erstellt und wird verwendet, um Ihre hochgeladenen Mediendateien zu speichern.



Verwalten von Buckets und Objekten

Dies sind die allgemeinen Schritte zur Verwaltung Ihres Lightsail-Objektspeicher-Buckets:

1. Erfahren Sie mehr über Objekte und Buckets im Amazon Lightsail-Objektspeicherdienst. Weitere Informationen finden Sie unter Objektspeicher in Amazon Lightsail.
2. Erfahren Sie mehr über die Namen, die Sie Ihren Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Regeln für die Bucket-Benennung in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherdienst, indem Sie einen Bucket erstellen. Weitere Informationen finden Sie unter Erstellen von Buckets in Amazon Lightsail.
4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren. Weitere Informationen finden Sie unter Bewährte Methoden für die Sicherheit von Amazon Lightsail-Objektspeichern und Grundlegendes zu Bucket-Berechtigungen in Amazon Lightsail.

   Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

   - Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail
   - Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail
   - Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
   - Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
   - Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail
   - Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail
5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.

   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherdienst
   - Zugriffsprotokollformat für einen Bucket im Amazon Lightsail-Objektspeicherdienst
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicherdienst
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail zum Identifizieren von Anforderungen

6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gibt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zur Verwaltung von Buckets in Amazon Lightsail .
7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unter Grundlegendes zu Objektschlüsselnamen in Amazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Hochladen von Dateien in einen Bucket in Amazon Lightsail
   - Hochladen von Dateien in einen Bucket in Amazon Lightsail mit mehrteiligem Upload
   - Anzeigen von Objekten in einem Bucket in Amazon Lightsail
   - Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
   - Herunterladen von Objekten aus einem Bucket in Amazon Lightsail
   - Filtern von Objekten in einem Bucket in Amazon Lightsail
   - Markieren von Objekten in einem Bucket in Amazon Lightsail
   - Löschen von Objekten in einem Bucket in Amazon Lightsail
9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.
10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.
11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.
12. Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen in Amazon Lightsail.
13. Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Plans Ihres Buckets in Amazon Lightsail.
14. Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.
   - Tutorial: Verbinden einer WordPress Instance mit einem Amazon Lightsail-Bucket

- Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Netzwerkverteilung für die Bereitstellung von Inhalten in Lightsail

15 Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

Konfigurieren Ihrer WordPress Instance für die Arbeit mit einer Netzwerkverteilung für die Bereitstellung von Inhalten in Lightsail

In diesem Leitfaden zeigen wir Ihnen, wie Sie Ihre WordPress Instance für die Arbeit mit einer Amazon Lightsail-Verteilung konfigurieren.

Für alle Lightsail-Verteilungen ist HTTPS standardmäßig für ihre Standarddomäne aktiviert (z. B. `123456abcdef.cloudfront.net`). Die Konfiguration Ihrer Verteilung bestimmt, ob die Verbindung zwischen Ihrer Verteilung und Ihrer Instance verschlüsselt ist.

- Ihre WordPress Website verwendet nur HTTP – Wenn Ihre Website nur HTTP als Ursprungsserver Ihrer Verteilung verwendet und nicht für die Verwendung von HTTPS konfiguriert ist, können Sie Ihre Verteilung so konfigurieren, dass SSL/TLS beendet und alle Inhaltsanfragen über eine unverschlüsselte Verbindung an Ihre Instance weitergeleitet werden.
- Ihre WordPress Website verwendet HTTPS – Wenn Ihre Website HTTPS als Ursprung Ihrer Verteilung verwendet, können Sie Ihre Verteilung so konfigurieren, dass alle Inhaltsanfragen über eine verschlüsselte Verbindung an Ihre Instance weitergeleitet werden. Diese Konfiguration wird als end-to-end Verschlüsselung bezeichnet.

Erstellen der Verteilung

Führen Sie die folgenden Schritte aus, um eine Lightsail-Verteilung für Ihre WordPress Instance zu konfigurieren. Weitere Informationen finden Sie unter the section called “Eine Verteilung erstellen”.

Voraussetzung

Erstellen und konfigurieren Sie eine WordPress Instance wie unter beschriebenthe section called “WordPress”.

So erstellen Sie eine Verteilung für Ihre WordPress Instance

1. Wählen Sie auf der Lightsail-Startseite Netzwerk aus.

2. Wählen Sie Verteilung erstellen aus.
3. Wählen Sie unter Ursprung auswählen die Region aus, in der Sie Ihre WordPress Instance ausführen, und wählen Sie dann Ihre WordPress Instance aus. Wir verwenden automatisch die statische IP-Adresse, die Sie an die Instance angehängt haben.
4. Wählen Sie für Caching-Verhalten die Option Optimal für aus WordPress.
5. (Optional) Um die end-to-end Verschlüsselung zu konfigurieren, ändern Sie die Ursprungsprotokollrichtlinie auf HTTPS only . Weitere Informationen finden Sie unter the section called “Ursprungsprotokollrichtlinie”.
6. Konfigurieren Sie die verbleibenden Optionen und wählen Sie dann Verteilung erstellen aus.
7. Wählen Sie auf der Registerkarte Benutzerdefinierte Domänen die Option Zertifikat erstellen aus. Geben Sie einen eindeutigen Namen für das Zertifikat ein, geben Sie die Namen Ihrer Domäne und Subdomänen ein und wählen Sie dann Zertifikat erstellen aus.
8. Wählen Sie Anfügen eines Zertifikatsaus.
9. Wählen Sie für DNS-Datensätze aktualisieren die Option Ich kenne .

Aktualisieren von DNS-Datensätzen

Führen Sie die folgenden Schritte aus, um die DNS-Datensätze für Ihre Lightsail-DNS-Zone zu aktualisieren.

So aktualisieren Sie die DNS-Datensätze für Ihre Verteilung

1. Wählen Sie auf der Lightsail-Startseite Domains und DNS aus.
2. Wählen Sie Ihre DNS-Zone und dann die Registerkarte DNS-Datensätze aus.
3. Löschen Sie die A- und AAAA-Datensätze für die Domäne, die Sie in Ihrem Zertifikat angegeben haben.
4. Wählen Sie Datensatz hinzufügen und erstellen Sie einen CNAME-Datensatz, der Ihre Domain in die Domain für Ihre Verteilung auflöst (z. B. d2vbec9EXAMPLE.cloudfront.net).
5. Wählen Sie Speichern.

Zulassen, dass statische Inhalte von der Verteilung zwischengespeichert werden

Führen Sie das folgende Verfahren aus, um die `wp-config.php` Datei in Ihrer WordPress Instance so zu bearbeiten, dass sie mit Ihrer Verteilung funktioniert.

> **Note**
>
> Wir empfehlen Ihnen, einen Snapshot Ihrer WordPress Instance zu erstellen, bevor Sie mit diesem Verfahren beginnen. Der Snapshot kann als Backup verwendet werden, aus dem Sie eine andere Instance erstellen können, falls etwas schief geht. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Linux- oder Unix-Instance.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite das browserbasierte SSH-Client-Symbol aus, das neben Ihrer Instance angezeigt wird WordPress .
3. Nachdem Sie mit Ihrer Instance verbunden sind, geben Sie den folgenden Befehl ein, um ein Backup der`wp-config.php` Datei zu erstellen. Wenn etwas schief geht, können Sie die Datei mithilfe des Backups wiederherstellen.

   ```
   sudo cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-
   config.php.backup
   ```

4. Geben Sie den folgenden Befehl ein, um die `wp-config.php`Datei mit Vim zu öffnen.

   ```
   sudo vim /opt/bitnami/wordpress/wp-config.php
   ```

5. Drücken Sie `I`, um den Einfügemodus in Vim einzugeben.
6. Löschen Sie die folgenden Codezeilen in der Datei.

   ```
   define('WP_SITEURL', 'http://' . $_SERVER['HTTP_HOST'] . '/');
   define('WP_HOME', 'http://' . $_SERVER['HTTP_HOST'] . '/');
   ```

7. Fügen Sie der Datei je nach verwendeter Version von eine der folgenden Codezeilen hinzu WordPress :

   - Wenn Sie Version 3.3 oder niedriger verwenden, fügen Sie den folgenden Codezeilen hinzu, in der Sie den Code zuvor gelöscht haben.

     ```
     define('WP_SITEURL', 'https://' . $_SERVER['HTTP_HOST'] . '/');
     define('WP_HOME', 'https://' . $_SERVER['HTTP_HOST'] . '/');
     if (isset($_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'])
     && $_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'] === 'https') {
     $_SERVER['HTTPS'] = 'on';
     ```

```
}
```

- Wenn Sie Version 3.3-1-5 oder höher verwenden, fügen Sie den folgenden Codezeilen hinzu, in der Sie den Code zuvor gelöscht haben.

```
define('WP_SITEURL', 'http://DOMAIN/');
define('WP_HOME', 'http://DOMAIN/');
if (isset($_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'])
&& $_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'] === 'https') {
$_SERVER['HTTPS'] = 'on';
}
```

8. Drücken Sie die Esc-Taste, um den Einfügemodus in Vim zu verlassen, geben Sie dann `:wq!` ein und drücken Sie die Enter-Taste, um Ihre Änderungen zu speichern (schreiben) und Vim zu beenden.
9. Geben Sie den folgenden Befehl ein, um den Apache-Dienst auf Ihrer Instance neu zu starten.

   ```
   sudo /opt/bitnami/ctlscript.sh restart apache
   ```

10. Warten Sie einige Augenblicke, bis der Apache-Dienst neu gestartet wird, und prüfen Sie dann, ob Ihre Verteilung Ihre Inhalte cached. Weitere Informationen finden Sie unter Testen Ihrer Amazon Lightsail-Verteilung.
11. Wenn etwas schief gelaufen ist, stellen Sie über den browserbasierten SSH-Client die Verbindung mit Ihrer Instance wieder her. Führen Sie den folgenden Befehl aus, um die `wp-config.php` Datei-Backup, die Sie zuvor in diesem Leitfaden erstellt haben, wiederherzustellen.

    ```
    sudo cp /opt/bitnami/wordpress/wp-config.php.backup /opt/bitnami/wordpress/wp-config.php
    ```

    Geben Sie nach der Wiederherstellung der Datei den folgenden Befehl ein, um den Apache-Service neu zu starten:

    ```
    sudo /opt/bitnami/ctlscript.sh restart apache
    ```

Zusätzliche Informationen über Verteilungen

Im Folgenden finden Sie einige Artikel, die Sie bei der Verwaltung von Verteilungen in Lightsail unterstützen:

- Netzwerkverteilungen für die Bereitstellung von Inhalten
- Erstellen von Verteilungen
- Verstehen von Anforderung- und Antwortverhalten einer Verteilung
- Testen Ihrer Verteilung
- Ändern des Ursprungs Ihrer Verteilung
- Ändern des Caching-Verhaltens Ihrer Verteilung
- Zurücksetzen des Caches Ihrer Verteilung
- Ändern des Plans Ihrer Verteilung
- Aktivieren benutzerdefinierter Domains für Ihre Verteilung
- Verweisen Ihrer Domain auf Ihre Verteilung
- Änderung benutzerdefinierter Domains für Ihre Verteilung
- Deaktivieren benutzerdefinierter Domains für die Verteilung
- Anzeigen von Verteilungsmetriken
- Löschen Ihrer Verteilung

Aktivieren Sie E-Mail auf Ihrer WordPress-Instance in Lightsail

Sie können E-Mail auf Ihrer WordPress-Instance in Amazon Lightsail aktivieren. Konfigurieren Sie den SMTP-Service im Amazon Simple Email Service (Amazon SES). Anschließend aktivieren und konfigurieren Sie das WP Mail SMTP-Plugin auf Ihrer Instance. Nachdem E-Mail aktiviert wurde, können Ihre WordPress-Administratoren das Zurücksetzen von Passwörtern für ihre Benutzerprofile beantragen und erhalten E-Mail-Benachrichtigungen zu Blog-Posts, Websiteaktualisierungen sowie andere Plugin-Nachrichten. In dieser Anleitung erfahren Sie, wie Sie E-Mail auf Ihrer WordPress-Instance in Amazon Lightsail mit Amazon SES aktivieren.

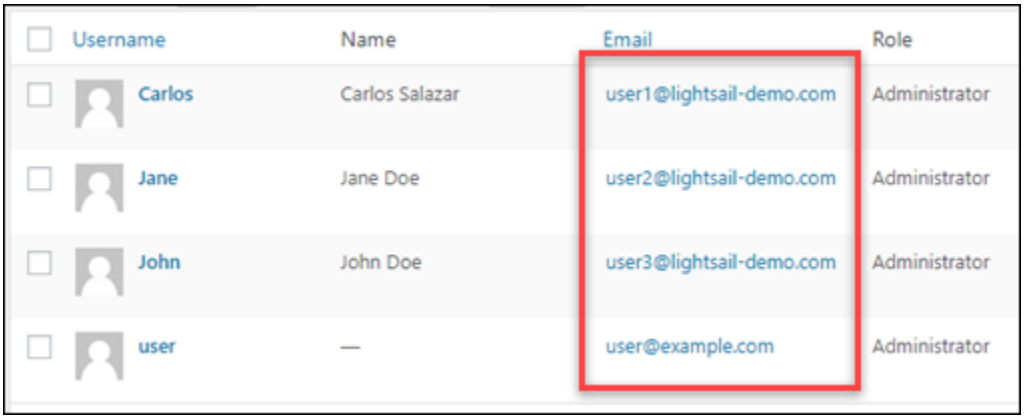
Inhalt

- Schritt 1: Überprüfen der Einschränkungen
- Schritt 2: Erfüllen der Voraussetzungen
- Schritt 3: Erstellen von SMTP-Anmeldeinformationen in Amazon SES
- Schritt 4: Überprüfen Ihrer Domain in Amazon SES
- Schritt 5: Verifizieren von E-Mail-Adressen in Amazon SES
- Schritt 6: Konfigurieren des WP Mail SMTP-Plug-Ins auf Ihrer WordPress-Instance

Weitere Informationen finden Sie unter Verwenden der Amazon-SES-SMTP-Benutzeroberfläche zum Senden von E-Mail in der Amazon-SES-Dokumentation.

Schritt 1: Überprüfen der Einschränkungen

Neue Amazon Web Services (AWS)-Konten, die sich in der Amazon-SES-Sandbox befinden, können E-Mails nur an verifizierte Adressen und Domains senden. Wenn dies für Ihr Konto der Fall ist, sollten Sie die Domäne Ihrer Website und die E-Mail-Adresse Ihrer WordPress-Administratoren überprüfen. Melden Sie sich zum Abrufen ihrer E-Mail-Adressen am Dashboard Ihrer WordPress-Website an, und wäglen Sie Users (Benutzer) im linken Navigationsmenü. Sie enthalten die Administrator-E-Mail-Adressen in der Spalte Email (E-Mail) aufgelistet, wie im folgenden Beispiel gezeigt:



> **Note**
>
> Das Standard-`user` Profil ist mit der `user@example.com`-E-Mail-Adresse konfiguriert. Sie sollten diese Einstellung zu einer funktionierenden E-Mail-Adresse ändern. Weitere Informationen finden Sie unter Benutzerprofilbildschirm in der WordPress-Dokumentation.

Um an eine beliebige Adresse und Domain E-Mail-Nachrichten senden zu können, müssen Sie beantragen, dass Ihr Konto aus der Amazon-SES-Sandbox genommen wird. Weitere Informationen finden Sie unter Verlassen der Amazon-SES-Sandbox in der Amazon-SES-Dokumentation.

Schritt 2: Erfüllen der Voraussetzungen

Sie müssen die folgenden Aufgaben ausführen, bevor Sie auf Ihrer WordPress-Instance E-Mail aktivieren können:

- Erstellen einer WordPress-Instance in Lightsail. Weitere Informationen finden Sie im Tutorial: Starten und Konfigurieren einer WordPress-Instance in Amazon Lightsail.

- Richten Sie die registrierte Domäne mithilfe einer Lightsail-DNS-Zone auf Ihre WordPress-Instance aus.. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.
- Melden Sie sich bei Amazon SES an und erfahren Sie mehr über den Service. Weitere Informationen zur Anmeldung für Amazon SES finden Sie unter Amazon-SES-Schnellstart in der Amazon-SES-Dokumentation. Weitere Informationen zu Amazon SES finden Sie in den folgenden Anleitungen in der Amazon-SES-Dokumentation.:
  - Entwicklerhandbuch für Amazon SES
  - Häufig gestellte Fragen zu Amazon SES
  - Amazon SES – Preise
  - Service Quotas für Amazon SES

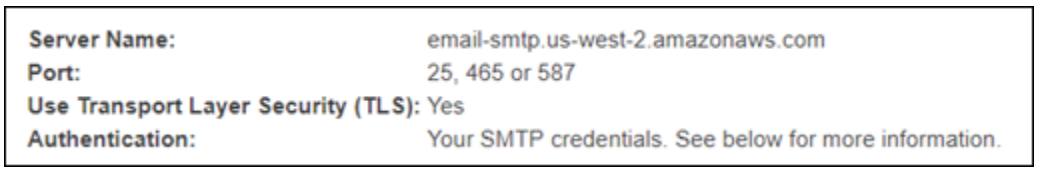
Schritt 3: Erstellen von SMTP-Anmeldeinformationen in Amazon SES

Das Erstellen von SMTP-Anmeldeinformationen in Ihrem Amazon-SES-Konto ist erforderlich, um das WP-Mail-SMTP-Plugin zu konfigurieren, das Sie später in diesem Leitfaden konfigurieren. Weitere Informationen finden Sie unter Abrufen Ihrer Amazon-SMTP-Anmeldeinformationen in der Amazon-SES-Dokumentation.

So erstellen Sie SMTP-Anmeldeinformationen in Amazon SES

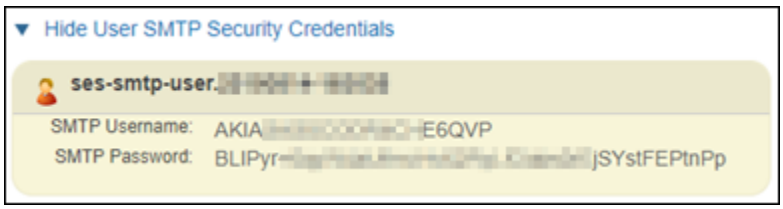
1. Melden Sie sich bei der Amazon-SES-Konsole an.
2. Wählen Sie im linken Navigationsmenü SMTP settings (SMTP-Einstellungen).

   Die Seite SMTP settings (SMTP-Einstellungen) zeigt Ihren SMTP-Server-Namen, die Ports und die TLS-Einstellung an. Notieren Sie diese Werte. Sie benötigen sie zu einem späteren Zeitpunkt in dieser Anleitung beim Konfigurieren des WP Mail SMTP-Plugins auf Ihrer WordPress-Instance.

3. Wählen Sie SMTP-Anmeldeinformationen erstellen.
4. Lassen Sie im Textfeld IAM-Benutzername den Standard-Benutzernamen stehen und wählen Sie dann Erstellen.

5. Wählen Sie die Option Show User SMTP Security Credentials (Benutzer-SMTP-Sicherheitsanmeldeinformationen anzeigen), um den SMTP-Benutzernamen und das Passwort anzuzeigen, oder Download Credentials (Anmeldeinformationen herunterladen) zum Herunterladen einer CSV-Datei mit den gleichen Informationen. Sie benötigen diese Anmeldeinformationen später beim Konfigurieren des WP Mail SMTP-Plugins auf Ihrer WordPress-Instance.



> **Note**
>
> Die Anmeldeinformationen, die in der Amazon-SES-Konsole erstellt wurden, werden automatisch zu AWS Identity and Access Management (IAM) für Ihr Konto hinzugefügt.

Schritt 4: Überprüfen Ihrer Domain in Amazon SES

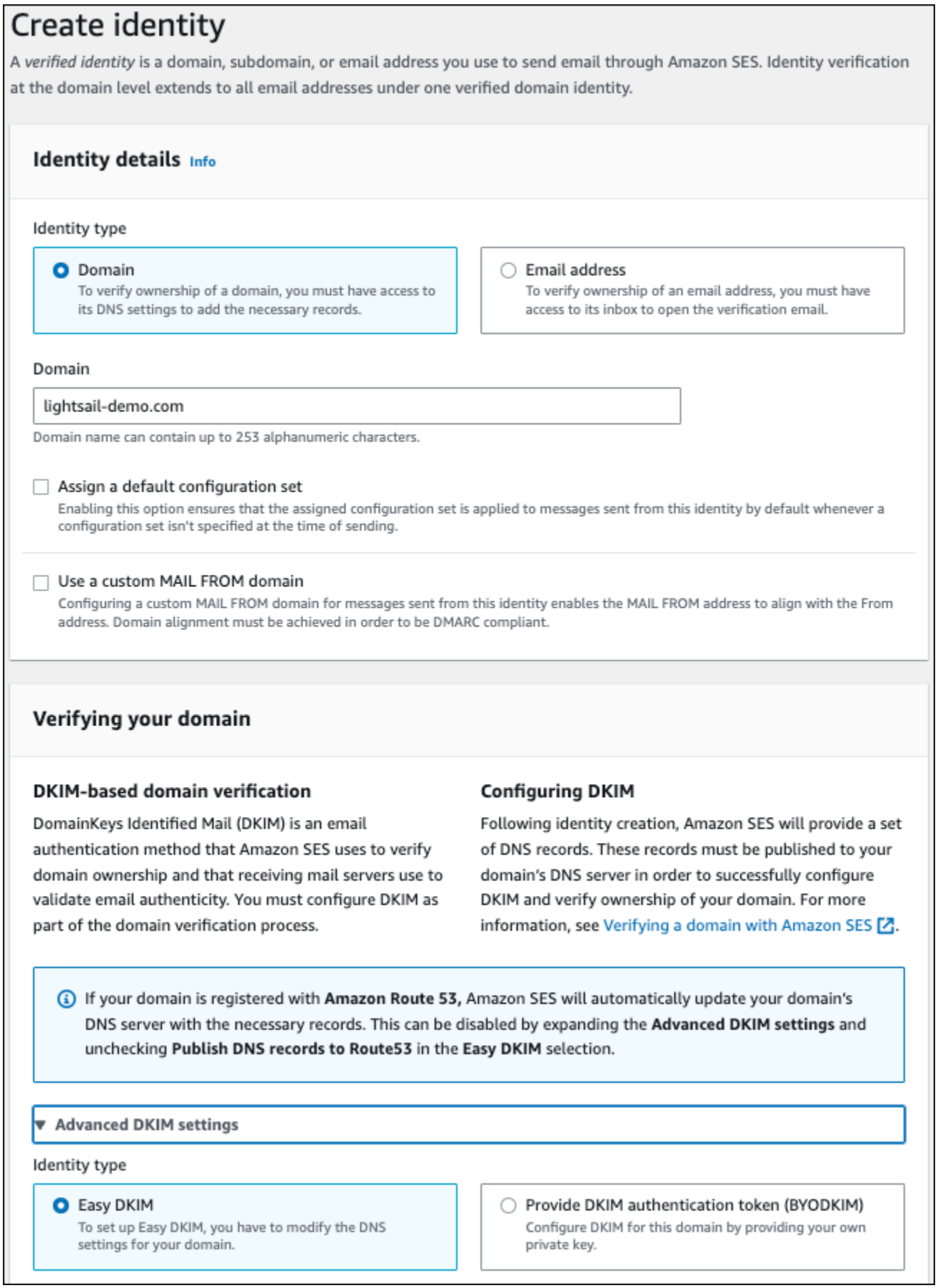
Amazon SES erfordert, dass Sie Ihre E-Mail-Adresse oder Domain verifizieren, um zu bestätigen, dass diese Ihnen gehört, und um zu vermeiden, dass sie von anderen verwendet wird. Wenn Sie eine Domäne verifizieren, verifizieren Sie alle E-Mail-Adressen dieser Domäne, so dass Sie diese nicht einzeln verifizieren müssen. Wenn Sie beispielsweise die Domäne `example.com` verifizieren, können Sie E-Mail-Nachrichten von `user1@example.com`, `user2@example.com` oder jedem anderen Benutzer unter `example.com` aus senden. Weitere Informationen finden Sie unter Verifizierung von Domains in Amazon SES in der Amazon-SES-Dokumentation.

So überprüfen Sie Ihre Domain in Amazon SES

1. Wählen Sie in der Amazon-SES-Konsole aus dem Navigationsmenü links die Option Verifizierte Domains aus.
2. Wählen Sie Create identity (Identität erstellen).
3. Geben Sie die Domain ein, die Sie verifizieren möchten, und wählen Sie Identität erstellen.

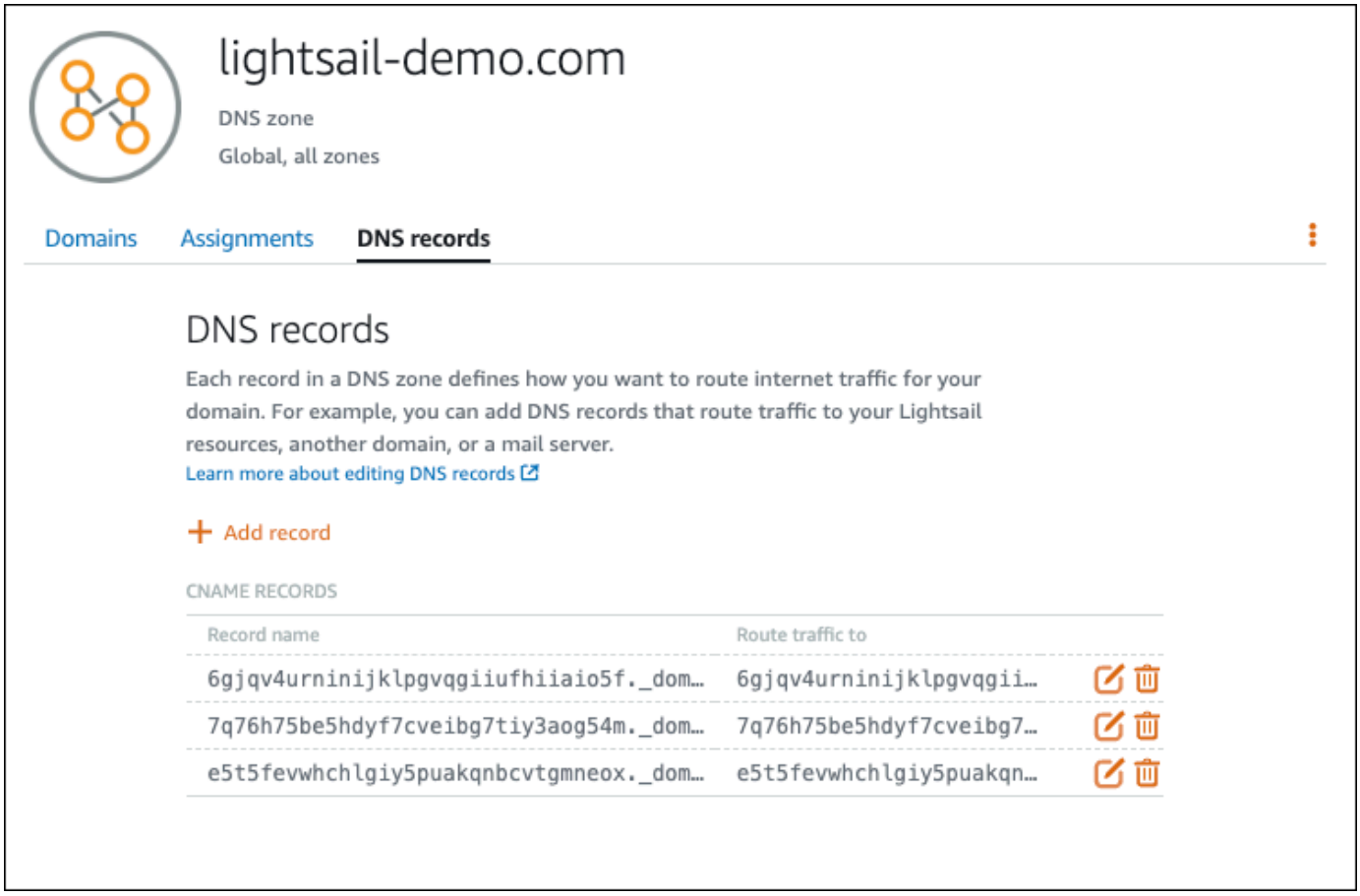
   Die Domäne, die Sie überprüfen, sollte die Domäne sein, die Sie mit Ihrer WordPress-Instance in Lightsail verwenden.

   > **Important**
   >
   > Legacy-TXT-Datensätze
   > Die Domain-Verifizierung in Amazon SES basiert nun auf DomainKeys Identified Mail (DKIM), einem E-Mail-Authentifizierungsstandard, den empfangende Mailserver verwenden, um die Authentizität einer E-Mail zu überprüfen. Durch die Konfiguration von DKIM in den DNS-Einstellungen Ihrer Domain wird SES bestätigt, dass Sie der Identitätsbesitzer sind, sodass keine TXT-Einträge erforderlich sind. Domain-Identitäten, die mithilfe von TXT-Einträgen verifiziert wurden, müssen nicht erneut verifiziert werden. Wir empfehlen jedoch dennoch, DKIM-Signaturen zu aktivieren, um die Zustellbarkeit Ihrer E-Mails bei DKIM-konformen E-Mail-Anbietern zu verbessern.


Create identity
A verified identity is a domain, subdomain, or email address you use to send email through Amazon SES. Identity verification at the domain level extends to all email addresses under one verified domain identity.
Identity details Info
Identity type
Domain
To verify ownership of a domain, you must have access to its DNS settings to add the necessary records.
Email address
To verify ownership of an email address, you must have access to its inbox to open the verification email.
Domain
lightsail-demo.com
Domain name can contain up to 253 alphanumeric characters.
Assign a default configuration set
Enabling this option ensures that the assigned configuration set is applied to messages sent from this identity by default whenever a configuration set isn't specified at the time of sending.
Use a custom MAIL FROM domain
Configuring a custom MAIL FROM domain for messages sent from this identity enables the MAIL FROM address to align with the From address. Domain alignment must be achieved in order to be DMARC compliant.
Verifying your domain
DKIM-based domain verification
DomainKeys Identified Mail (DKIM) is an email authentication method that Amazon SES uses to verify domain ownership and that receiving mail servers use to validate email authenticity. You must configure DKIM as part of the domain verification process.
Configuring DKIM
Following identity creation, Amazon SES will provide a set of DNS records. These records must be published to your domain's DNS server in order to successfully configure DKIM and verify ownership of your domain. For more information, see Verifying a domain with Amazon SES.
If your domain is registered with Amazon Route 53, Amazon SES will automatically update your domain's DNS server with the necessary records. This can be disabled by expanding the Advanced DKIM settings and unchecking Publish DNS records to Route53 in the Easy DKIM selection.
Advanced DKIM settings
Identity type
Easy DKIM
To set up Easy DKIM, you have to modify the DNS settings for your domain.
Provide DKIM authentication token (BYODKIM)
Configure DKIM for this domain by providing your own private key.

4. Nachdem Sie Ihre Domain-Identität mit Easy DKIM erstellt haben, müssen Sie den Verifizierungsprozess mit DKIM-Authentifizierung abschließen, indem Sie die folgenden generierten CNAME-Einträge kopieren, um sie beim DNS-Anbieter Ihrer Domain zu veröffentlichen. Die Erkennung dieser Aufzeichnungen kann bis zu 72 Stunden dauern. Weitere Informationen finden Sie unter Überprüfen einer Domain-Identität mit DKIM und Easy DKIM
5. Öffnen Sie ein neues Browserfenster und navigieren Sie zu der Lightsail-Konsole.
6. Wählen Sie auf der Lightsail-Startseite Domains und DNS und dann die DNS-Zone Ihrer Domain aus.
7. Fügen Sie die DNS-Datensätze aus der Amazon-SES-Konsole hinzu. Weitere Informationen zum Bearbeiten einer DNS-Zone in Lightsail finden Sie unter Bearbeiten einer DNS-Zone in Amazon Lightsail.

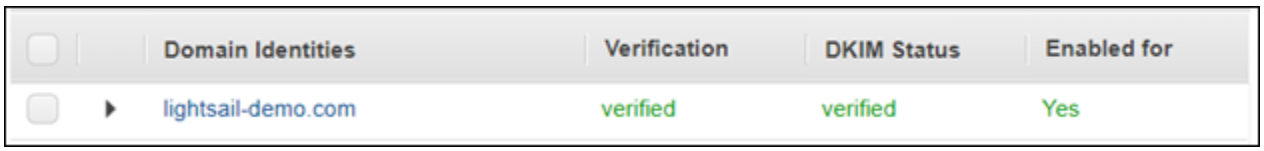
   Das Ergebnis sollte wie folgt aussehen:



> **Note**
>
> Geben Sie ein @-Symbol in das Textfeld Subdomain (Subdomäne) zur Verwendung des Apex Ihrer Domäne für einen MX-Datensatz ein. Darüber hinaus ist der von Amazon SES bereitgestellte MX-Datensatzwert `10 inbound-smtp.us-west-2.amazonaws.com`. Geben Sie `10` als Priority (Priorität)- und `inbound-smtp.us-west-2.amazonaws.com` als Maps to (Verweist auf)-Domäne an.

8. Schließen Sie in der Amazon-SES-Konsole die Seite Eine neue Domain verifizieren.

   Nach einigen Minuten wird Ihre Domain in der Amazon-SES-Konsole als bestätigt und zum Senden aktiviert angezeigt, wie im folgenden Beispiel gezeigt:



   Ihr SMTP-Service in Amazon SES ist jetzt bereit, E-Mail-Nachrichten von Ihrer Domain zu senden.

Schritt 5: Verifizieren von E-Mail-Adressen in Amazon SES

Als neuer Amazon-SES-Kunde müssen Sie die E-Mail-Adressen, an die Sie E-Mail-Nachrichten senden möchten, verifizieren. Dazu fügen Sie die E-Mail-Adressen in der Amazon-SES-Konsole hinzu. Weitere Informationen finden Sie unter Verifizierung von E-Mail-Adressen in Amazon SES in der Amazon-SES-Dokumentation.

Wir empfehlen, dass Sie die E-Mail-Adressen Ihrer WordPress-Website-Administratoren hinzufügen. Auf diese Weise können diese Passwortzurücksetzungen für ihre Benutzerprofile anfordern und E-Mail-Benachrichtigungen zu Blog-Posts, Website-Updates und andere Plugin-Nachrichten erhalten.

> **Note**
>
> Wenn Sie E-Mail-Nachrichten ohne Verifizierung an beliebige Adressen senden möchten, müssen Sie Ihr Amazon-SES-Konto aus der Sandbox nehmen. Weitere Informationen finden Sie unter Verlassen der Amazon-SES-Sandbox in der Amazon-SES-Dokumentation.

Erstellen einer E-Mail-Adressidentität

1. Wählen Sie in der Amazon-SES-Konsole aus dem Navigationsmenü links die Option Verifizierte Domains aus.
2. Wählen Sie Create identity (Identität erstellen).
3. Wählen Sie E-Mail-Adresse. Geben Sie die E-Mail-Adresse ein, die Sie verifizieren möchten.
4. Wählen Sie Create identity (Identität erstellen).

Wiederholen Sie die Schritte 1 bis 4 für jede E-Mail-Adresse, die Sie verifizieren möchten. Eine Bestätigungs-E-Mail-Nachricht wird an die E-Mail-Adresse gesendet, die Sie eingegeben haben. Die Adresse wird der Liste der verifizierten E-Mail-Identitäten mit dem Status „Pending verification (Verifizierung ausstehend)“ hinzugefügt. Sie wird als „verified (verifiziert)“ markiert, wenn der Benutzer die E-Mail-Nachricht geöffnet und den Verifizierungsprozess abgeschlossen hat.

So verifizieren Sie die Identität einer E-Mail-Adresse

1. Suchen Sie im Posteingang der eingegebenen Adresse nach einer E-Mail von no-reply-aws@amazon.com.
2. Öffnen Sie die E-Mail und klicken Sie auf den Link in der E-Mail, um die Verifizierung der E-Mail-Adresse abzuschließen. Nachdem es abgeschlossen ist, wird Status auf Verified (Bestätigt) aktualisiert.

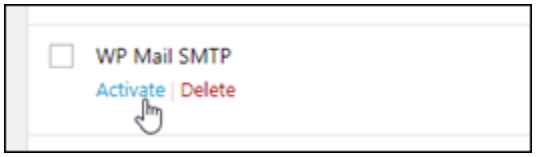
Schritt 6: Konfigurieren des WP Mail SMTP-Plug-Ins auf Ihrer WordPress-Instance

Der letzte Schritt ist die Konfiguration des WP Mail SMTP-Plugins auf Ihrer WordPress-Instance. Verwenden Sie die SMTP-Anmeldeinformationen, die Sie zuvor erstellt haben, in der Amazon-SES-Konsole.

So konfigurieren Sie das WP Mail SMTP-Plugin auf Ihrer WordPress-Instance:

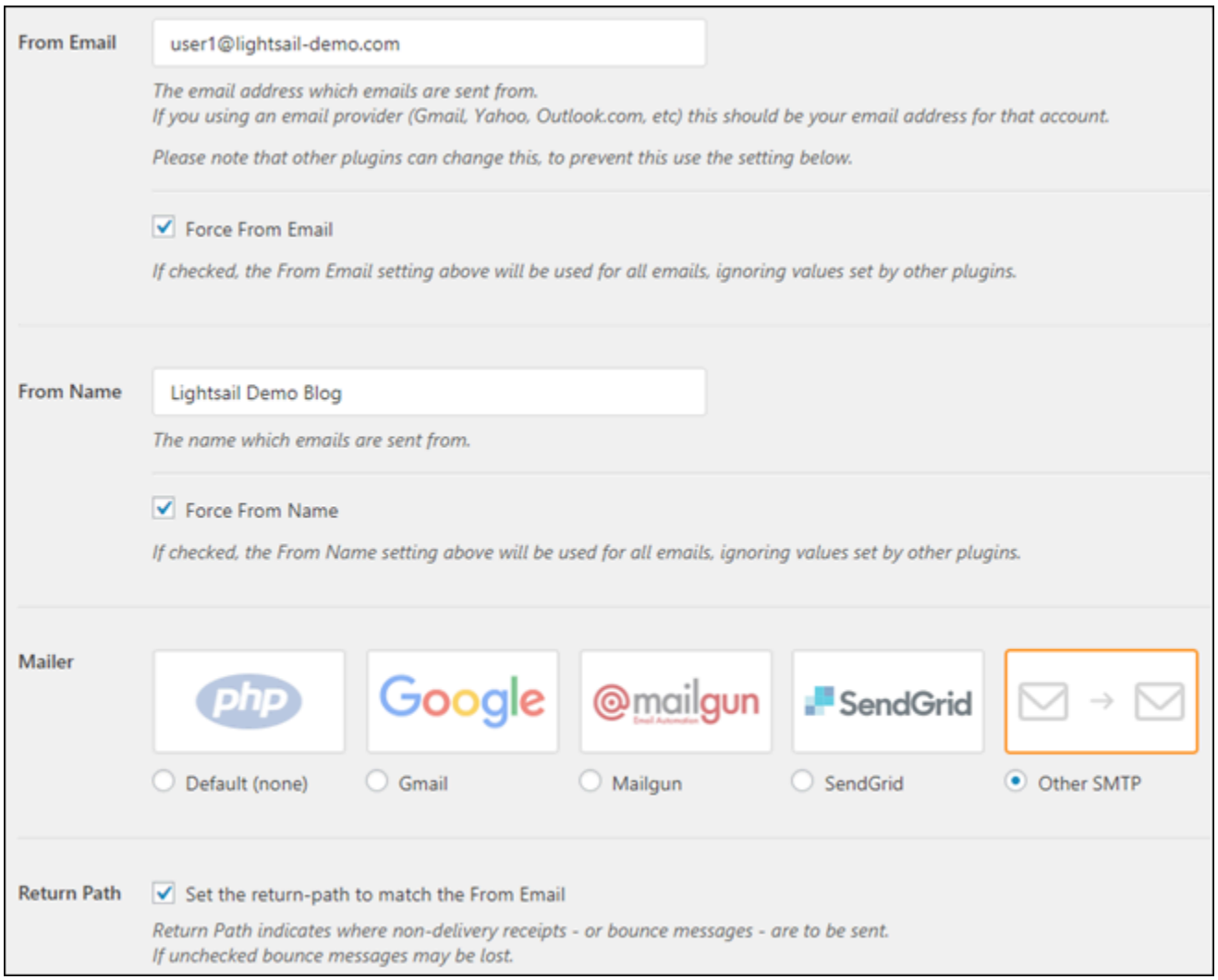
1. Melden Sie sich beim Dashboard Ihrer WordPress-Website als Administrator an.

2. Wählen Sie im linken Navigationsmenü Plugins und klicken Sie dann auf Installed Plugins (Installierte Plugins).
3. Führen Sie einen Bildlauf nach unten zum WP Mail SMTP-Plugin durch und klicken Sie dann auf Activate (Aktivieren). Wenn eine neue Version des Plugins vorhanden ist, stellen Sie sicher, dass Sie das Plugin aktualisieren, bevor Sie mit dem nächsten Schritt fortfahren.

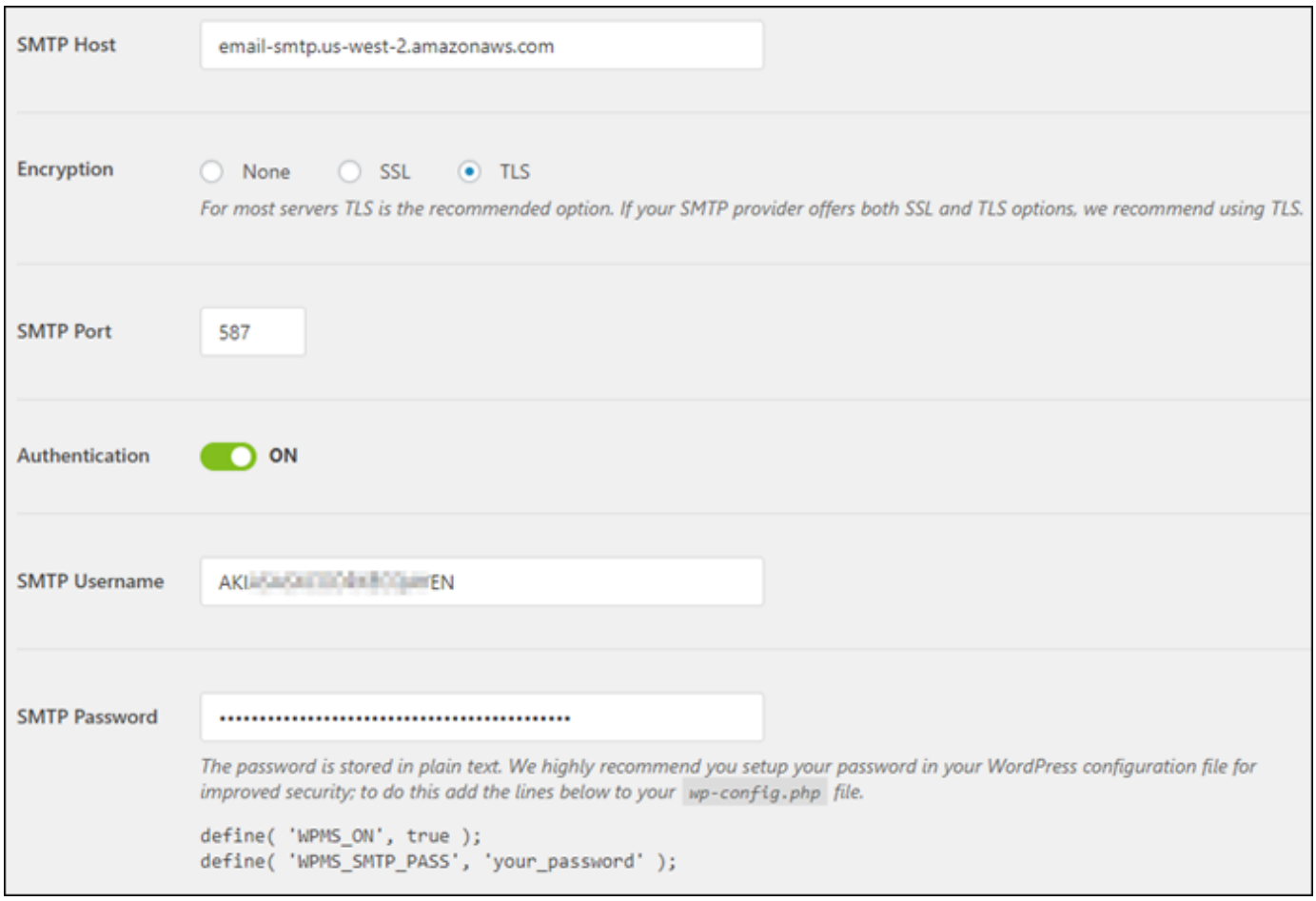


4. Nachdem das WP Mail SMTP-Plugin aktiviert ist, wählen Sie Settings (Einstellungen). Möglicherweise müssen Sie einen Bildlauf nach unten zum Suchen des Plugins duchführen.

5. Geben Sie im Textfeld From Email Address (Von-E-Mail-Adresse) die E-Mail-Adresse ein, von der die E-Mail-Nachrichten aus gesendet werden sollen. Die E-Mail-Adresse, die Sie eingeben, muss in Amazon SES anhand der vorher erläuterten Schritte bestätigt werden.
6. Wählen Sie Force From Email (Von-E-Mail erzwingen), um die Verwendung der E-Mail-Adresse zu erzwingen, die Sie im Textfeld From Email Address (Von-E-Mail-Adresse) eingegeben haben und die „Von-E-Mail-Adresse“ zu ignorieren, die von anderen plugins eingerichtet wurde.
7. Geben Sie im Textfeld From Name (Absendername) den Namen an, der der Absender der E-Mail-Nachrichten sein soll, oder lassen Sie ihn unverändert, damit der Name des WordPress-Blogs verwendet wird.
8. Wählen Sie Force From Name (Absendername erzwingen), um die Verwendung des Namens zu erzwingen, den Sie im Textfeld From Name (Absendername) eingegeben haben. Wenn Sie diese Option wählen, wird der Wert für „Absendername“, der von anderen Plugins eingerichtet wurde, ignoriert, und WordPress verwendet den Namen, den Sie in dem Textfeld From Name (Absendername) eingegeben haben.
9. Wählen Sie im Mailer-Abschnitt der Seite Other SMTP (Anderes SMTP).
10. Wäglen Sie Set the return-path to match the From Email (Antwortpfad an Von-E-Mail-Adresse anpassen), damit Nichtzustellbarkeitsmeldungen an die E-Mail-Adresse gesendet werden, die Sie im Textfeld From Email Address (Von-E-Mail-Adresse) eingegeben haben.



11. Geben Sie im Textfeld SMTP-Host den SMTP-Server-Namen ein, den Sie weiter oben in dieser Anleitung über die Seite SMTP-Einstellungen in der Amazon-SES-Konsole erhalten haben.
12. Wählen Sie TLS im Bereich Verschlüsselung der Seite, um anzugeben, dass der SMTP-Service in Amazon SES die TLS-Verschlüsselung verwendet.
13. Lassen Sie im Textfeld SMTP Port den Standardwert 587 unverändert.
14. Schalten Sie die Authentifizierung auf EIN und geben Sie dann den SMTP-Benutzernamen und das Passwort ein, die Sie weiter oben in dieser Anleitung aus der Amazon-SES-Konsole erhalten haben.

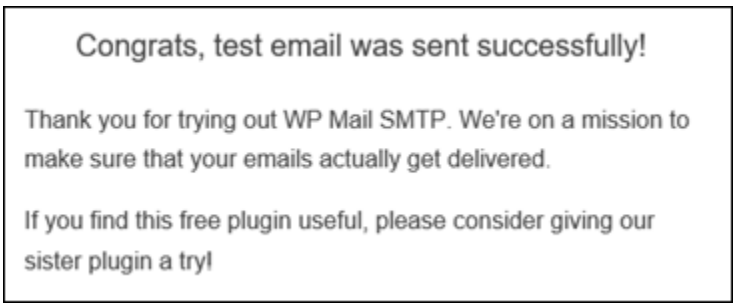


15. Wählen Sie Save settings (Einstellungen speichern). Sie sehen eine Bestätigung, dass die Einstellungen erfolgreich gespeichert wurden.
16. Wählen Sie die Registerkarte EmailTest (E-Mail-Test).

    Im nächsten Schritt senden Sie eine Test-E-Mail-Nachricht, um zu bestätigen, dass der E-Mail-Service funktioniert.
17. Geben Sie eine E-Mail-Adresse in das Textfeld Send To (Senden an) ein und klicken Sie dann auf Send Email (E-Mail-Nachricht senden). Die E-Mail-Adresse, die Sie eingeben, muss in Amazon SES anhand der vorher erläuterten Schritte bestätigt werden.

    Es gibt zwei mögliche Ergebnisse, die Sie sehen können.

    - Wenn Sie eine Erfolgsbestätigung sehen, ist Ihre WordPress-Website für E-Mail aktiviert. Vergewissern Sie sich, dass die folgende Test-E-Mail im angegebenen Postfach eingetroffen ist:



Sie können jetzt die Option Lost your password? (Passwort vergessen?) auf der Anmeldeseite für das Dashboard Ihrer WordPress-Website wählen. Ein neues Passwort wird Ihnen per E-Mail zugestellt, wenn die E-Mail-Adresse in Ihrem WordPress-Benutzerprofil in Amazon SES bestätigt ist.

- Wenn Sie eine Fehlermeldung erhalten, prüfen Sie, ob die im WP-Mail-SMTP-Plugin eingegebenen SMTP-Einstellungen denen des SMTP-Service in Ihrem Amazon-SES-Konto entsprechen. Vergewissern Sie sich außerdem, dass Sie eine E-Mail-Adresse verwenden, die Sie in Amazon SES verifiziert haben.

Aktivieren Sie HTTPS auf Ihrer WordPress Instanz in Lightsail

Wenn Sie Hypertext Transfer Protocol Secure (HTTPS) für Ihre WordPress Website aktivieren, können Besucher sicher sein, dass Ihre Website sicher ist und dass verschlüsselte Daten gesendet und empfangen werden. Eine nicht sichere Website hat eine Adresse, die mit `http`, wie beispielsweise`http://example.com`, während eine sichere Website eine Adresse hat, die mit `https`, wie beispielsweise `https://example.com` beginnt. Auch wenn Ihre Website primär informativ ist, wird dennoch empfohlen, HTTPS zu aktivieren. Dies liegt daran, dass die meisten Webbrowser, Website-Besucher darüber informieren, dass Ihre Website nicht sicher ist, wenn HTTPS nich aktiviert ist, und Ihre Website wird niedriger bei Suchergebnissen von Suchmaschinen eingeordnet.

> **Tip**
>
> Lightsail bietet einen geführten Workflow, der die Installation und Konfiguration eines SSL-/TLS-Let's Encrypt-Zertifikats auf Ihrer Instanz automatisiert. WordPress Wir empfehlen Ihnen dringend, den Workflow zu verwenden, anstatt die manuellen Schritte in diesem Tutorial zu befolgen. Weitere Informationen finden Sie unter Starten und Konfigurieren einer WordPress Instanz.

Diese Anleitung zeigt Ihnen, wie Sie das Bitnami HTTPS-Konfigurationstool (`bncert`) verwenden, um HTTPS auf Ihrer Certified by WordPress Bitnami-Instance auf Amazon Lightsail zu aktivieren. Damit können Sie Zertifikate nur für die Domänen und Unterdomänen anfordern, die Sie bei der Anforderung angeben. Alternativ, können Sie mit dem Certbot-Tool ein einzelnes Zertifikat für eine Domain und ein Platzhalterzertifikat für Subdomains anfordern. Ein Platzhalterzertifikat funktioniert fürjegliche Unterdomänen einer Domäne, was von Vorteil ist, wenn Sie nicht wissen, welche Unterdomänen Sie verwenden werden, um den Datenverkehr auf Ihre Instance zu leiten. Certbot erneuert Ihr Zertifikat jedoch nicht automatisch wie das `bncert`-Tool. Wenn Sie Certbot verwenden, müssen Sie Ihre Zertifikate alle 90 Tage manuell erneuern. Weitere Informationen zur Verwendung von Certbot zur Aktivierung von HTTPS finden Sie unter Tutorial: Verwenden Sie Let's Encrypt SSL-Zertifikate mit Ihrer Instance. WordPress

Inhalt

Schritt 1: Weitere Informationen über den Prozess

> **Note**
>
> In diesem Abschnitt erhalten Sie einen hochgradigen Überblick über den Prozess. Die spezifischen Schritte zur Durchführung dieses Prozesses sind in den nachfolgenden Schritten dieses Leitfadens enthalten.

Um HTTPS für Ihre WordPress Website zu aktivieren, stellen Sie über SSH eine Verbindung zu Ihrer Lightsail-Instanz her und fordern Sie mit dem `bncert` Tool ein SSL/TLS-Zertifikat von der Let's Encrypt-Zertifizierungsstelle an. Wenn Sie das Zertifikat anfordern, geben Sie die primäre Domäne Ihrer Website an (`example.com`) und alternative Domänen (`www.example.com`,`blog.example.com`usw.), falls vorhanden. Let‘s Encrypt validiert, ob Sie Eigentümer der Domänen sind, indem Sie entweder aufgefordert werden, TXT-Akten im DNS Ihrer

Domänen zu erstellen, oder indem Sie überprüfen, ob diese Domänen bereits Datenverkehr an die öffentliche IP-Adresse der Instance weiterleiten, von der Sie die Anforderung stellen.

Nachdem Ihr Zertifikat validiert wurde, können Sie Ihre WordPress Website so konfigurieren, dass Besucher automatisch von HTTP zu HTTPS umgeleitet werden (`http://example.com`Weiterleitungen zu`https://example.com`), sodass Besucher gezwungen sind, die verschlüsselte Verbindung zu verwenden. Sie können Ihre Website auch so konfigurieren, dass die`www`Unterdomänen automatisch auf die Spitze Ihrer Domäne (`https://www.example.com` Umleitung auf `https://example.com`) oder umgekehrt (`https://example.com` Umleitung auf`https://www.example.com`) umleiten. Diese Umleitungen werden auch mit dem`bncert`-Tool konfiguriert.

Let's Encrypt verlangt, dass Sie Ihr Zertifikat alle 90 Tage erneuern, um HTTPS auf Ihrer Website zu behalten. Das `bncert`-Tool erneuert automatisch Ihre Zertifikate für Sie, sodass Sie mehr Zeit damit verbringen können, sich auf Ihre Website zu konzentrieren.

Einschränkungen des bncert-Tools

Für das `bncert`-Tool gelten folgende Einschränkungen:

- Es ist nicht auf allen Certified by WordPress Bitnami-Instanzen vorinstalliert, wenn sie erstellt werden. WordPress Für Instanzen, die vor einiger Zeit auf Lightsail erstellt wurden, müssen Sie das Tool manuell installieren. `bncert` Schritt 4 dieses Leitfadens zeigt, wie Sie bestätigen, dass das Tool auf Ihrer Instance installiert ist und wie Sie es installieren, falls dies nicht der Fall ist.
- Damit können Sie Zertifikate nur für die Domains und Unterdomains anfordern, die Sie bei der Anforderung angeben. Dies ist anders als das Certbot-Tool, welches Ihnen ermöglicht, ein Zertifikat für Domain und ein Platzhalterzertifikat für Subdomains anzufordern. Ein Platzhalterzertifikat funktioniert fürjegliche Unterdomänen einer Domäne, was von Vorteil ist, wenn Sie nicht wissen, welche Unterdomänen Sie verwenden werden, um den Datenverkehr auf Ihre Instance zu leiten. Certbot erneuert Ihr Zertifikat jedoch nicht automatisch wie das `bncert`-Tool. Wenn Sie Certbot verwenden, müssen Sie Ihre Zertifikate alle 90 Tage manuell erneuern. Weitere Informationen zur Verwendung von Certbot zur Aktivierung von HTTPS finden Sie unter Tutorial: Let's Encrypt SSL-Zertifikate mit Ihrer WordPress Instance in Amazon Lightsail verwenden.

Schritt 2: Erfüllen der Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies nicht ohnehin bereits der Fall ist:

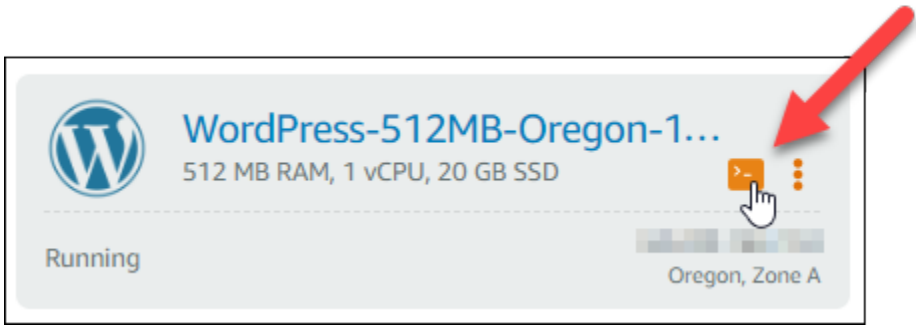
- Erstellen Sie eine WordPress Instanz in Lightsail und konfigurieren Sie Ihre Website auf Ihrer Instanz. Weitere Informationen finden Sie unter Erste Schritte mit Linux/UNIX-basierten Instances in Amazon Lightsail.
- Fügen Sie Ihrer Instance eine statische IP an. Die öffentliche IP-Adresse Ihrer Instance ändert sich, wenn Sie Ihre Instance stoppen und starten. Eine statische IP-Adresse ändert sich nicht, wenn Sie Ihre Instance stoppen und starten. Weitere Informationen finden Sie unter Erstellen Sie eine statische IP-Adresse und fügen Sie sie an eine Instance in Amazon Lightsail an.
- Erstellen Sie einen Snapshot Ihrer WordPress Instance, nachdem Sie sie konfiguriert haben, oder aktivieren Sie automatische Snapshots. Der Snapshot kann als Backup verwendet werden, aus dem Sie eine andere Instance erstellen können, falls etwas mit Ihrer Ursprungs-Instance schief geht. Weitere Informationen finden Sie unter Erstellen eines Snapshots Ihrer Linux- oder Unix-Instance oder Aktivieren oder Deaktivieren von automatischen Snapshots für Instances oder Festplatten in Amazon Lightsail.
- Fügen Sie DNS-Einträge zum DNS Ihrer Domain hinzu, die den Traffic für den Apex Ihrer Domain (`example.com`) und für deren `www` Subdomain (`www.example.com`) an die öffentliche IP-Adresse Ihrer WordPress Instance in Lightsail weiterleiten. Sie können diese Aktionen beim aktuellen DNS-Hostinganbieter Ihrer Domäne ausführen. Oder wenn Sie die Verwaltung des DNS Ihrer Domain an Lightsail übertragen haben, können Sie diese Aktionen mithilfe einer DNS-Zone in Lightsail durchführen. Weitere Informationen hierzu finden Sie unter DNS.

> **Important**
>
> Fügen Sie DNS-Einträge zum DNS aller Domains hinzu, die Sie mit Ihrer Website verwenden möchten. WordPress Alle diese Domains sollten den Verkehr an die öffentliche IP-Adresse Ihrer WordPress Website weiterleiten. Das `bncert` Tool stellt Zertifikate nur für Domains aus, die derzeit Traffic an die öffentliche IP-Adresse Ihrer WordPress Instance weiterleiten.

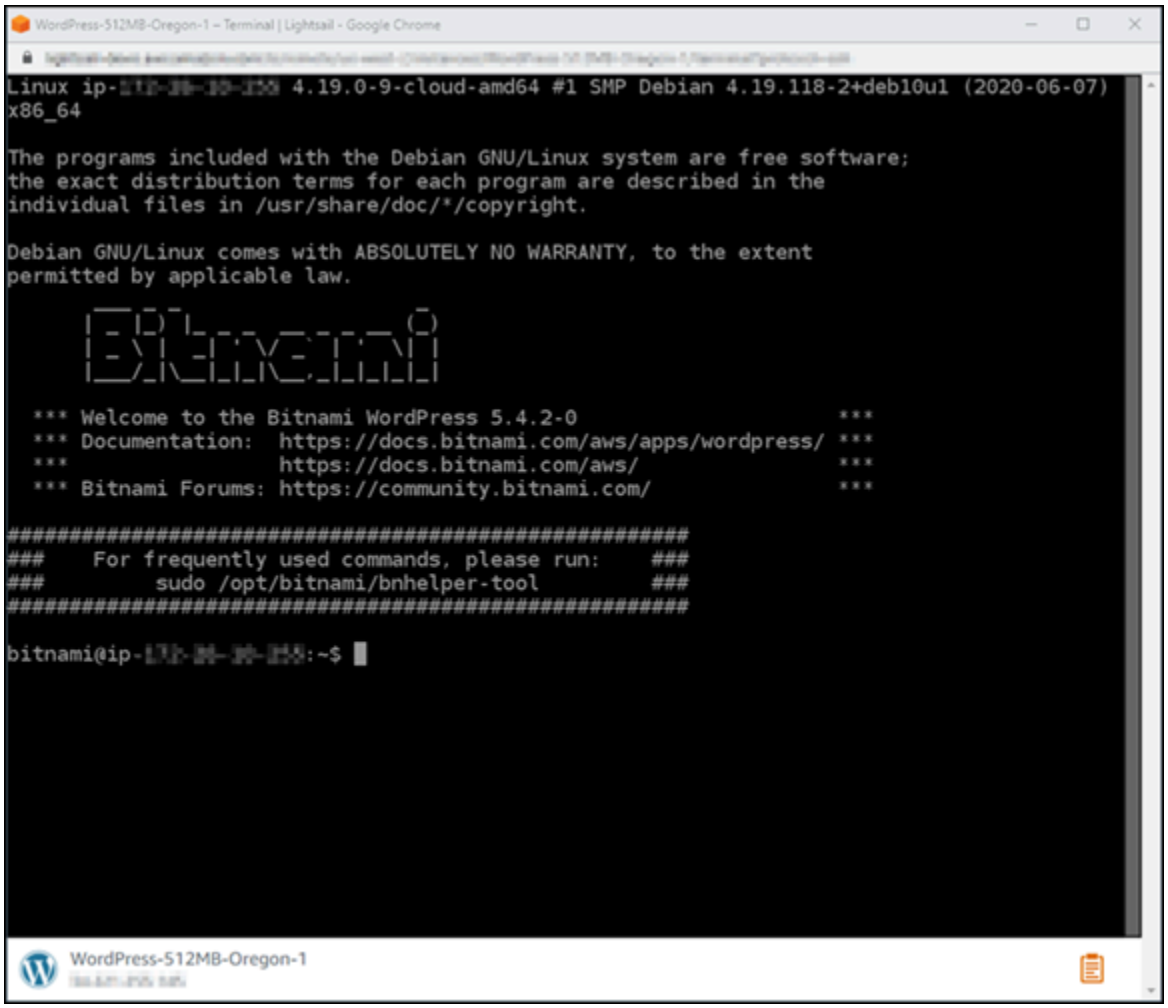
Schritt 3: Verbindung mit Ihrer Instance herstellen

Führen Sie die folgenden Schritte aus, um mithilfe des browserbasierten SSH-Clients in der Lightsail-Konsole eine Verbindung zu Ihrer Instance herzustellen.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite das SSH-Schnellverbindungssymbol für Ihre Instance aus. WordPress



Das Terminalfenster des browserbasierten SSH-Clients wird geöffnet. Sie sind erfolgreich über SSH mit Ihrer Instance verbunden, wenn Sie das Bitnami-Logo sehen, wie im folgenden Beispiel gezeigt.



Schritt 4: Bestätigen Sie, dass das bncert-Tool auf Ihrer Instance installiert ist

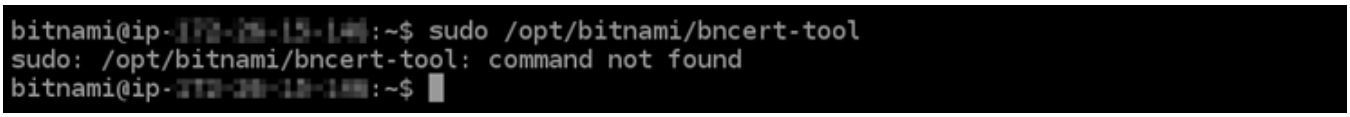
Vervollständigen Sie die folgenden Schritte, um sicherzustellen, dass das Bitnami-HTTPS-Konfigurationstool (`bncert`) auf Ihrer Instance installiert ist. Es ist nicht auf allen Certified by WordPress Bitnami-Instanzen vorinstalliert, wenn sie erstellt werden. WordPress Für Instanzen, die vor einiger Zeit auf Lightsail erstellt wurden, müssen Sie das Tool manuell installieren. `bncert` Dieses Verfahren beinhaltet die Schritte, um das Tool zu installieren, wenn es nicht installiert ist.

1. Geben Sie den folgenden Befehl ein, um das `bncert`-Tool auszuführen.

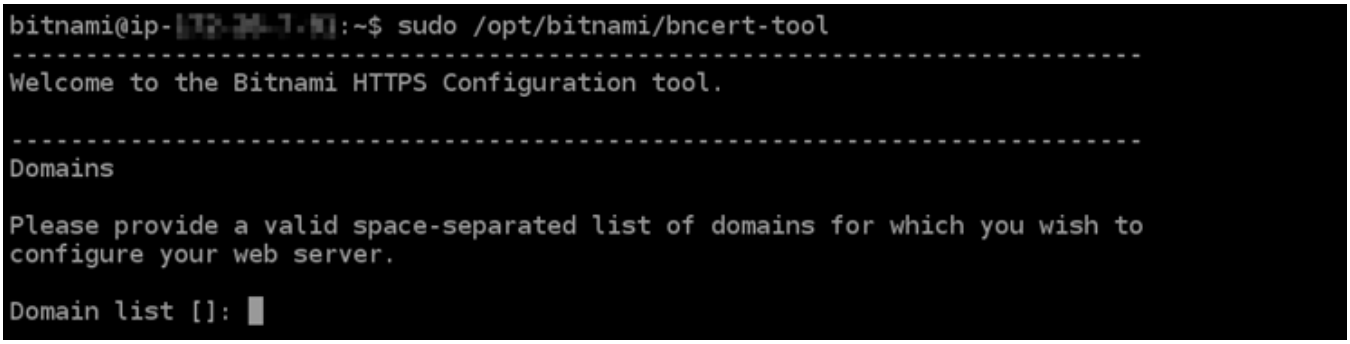
   ```
   sudo /opt/bitnami/bncert-tool
   ```

   - Wenn Sie `command not found`, wie in der Antwort im folgenden Beispiel gezeigt, sehen, ist das `bncert`-Tool auf Ihrer Instance nicht installiert. Fahren Sie mit dem nächsten Schritt in diesem Verfahren fort, um das `bncert`-Tool auf Ihrer Instance zu installieren.

     > **Important**
     >
     > Das `bncert` Tool kann nur auf WordPress Instanzen verwendet werden, die von Bitnami zertifiziert sind. Alternativ können Sie das Certbot-Tool verwenden, um HTTPS auf Ihrer Instance zu aktivieren. WordPress Weitere Informationen finden Sie unter Tutorial: Verwenden Sie Let's Encrypt SSL-Zertifikate mit Ihrer Instance. WordPress

   - Wenn Sie `Welcome to the Bitnami HTTPS configuration tool`, wie in der Antwort im folgenden Beispiel gezeigt, sehen, ist das `bncert`-Tool auf Ihrer Instance installiert. Fahren Sie mit dem Abschnitt Schritt 5: HTTPS auf Ihrer WordPress Instance aktivieren in diesem Handbuch fort.



2. Geben Sie den folgenden Befehl ein, um die `bncert` Laufdatei auf Ihre Instance herunterzuladen.

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/bncert-linux-x64.run
```

3. Geben Sie den folgenden Befehl ein, um ein Verzeichnis für die`bncert` Laufdatei auf Ihrer Instance zu erstellen.

```
sudo mkdir /opt/bitnami/bncert
```

4. Geben Sie den folgenden Befehl ein, um die heruntergeladene `bncert` Laufdatei in das neue Verzeichnis zu verschieben, das Sie erstellt haben.

```
sudo mv bncert-linux-x64.run /opt/bitnami/bncert/
```

5. Geben Sie den folgenden Befehl ein, um die `bncert` Laufdatei als ein Programm auszuführen.

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. Geben Sie den folgenden Befehl ein, um einen symbolischen Link zu erstellen, der das`bncert`-Tool ausführt, wenn Sie den `sudo /opt/bitnami/bncert-tool`-Befehl eingeben.

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

Sie sind jetzt fertig mit der Installation des `bncert`-Tools auf Ihrer Instance. Fahren Sie mit dem Abschnitt Schritt 5: HTTPS auf Ihrer WordPress Instance aktivieren in diesem Handbuch fort.

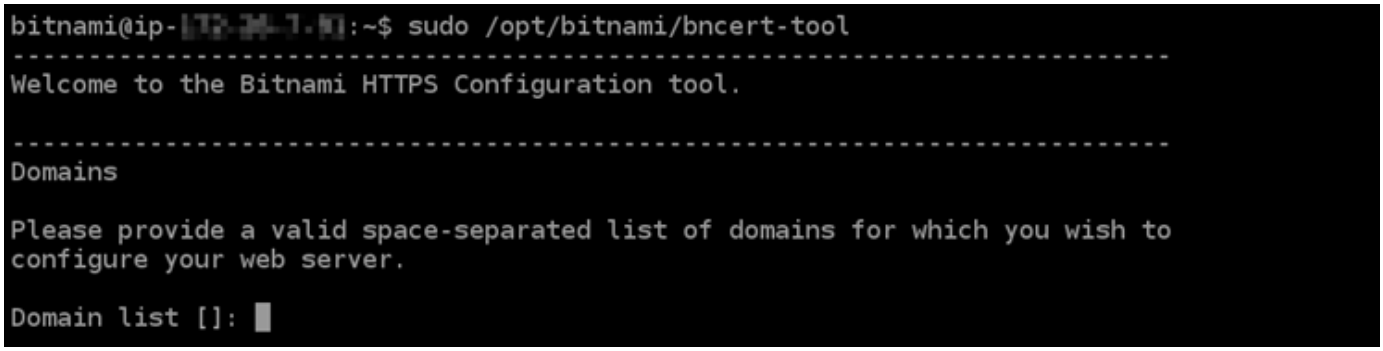
Schritt 5: Aktivieren Sie HTTPS auf Ihrer WordPress Instance

Gehen Sie wie folgt vor, um HTTPS auf Ihrer WordPress Instance zu aktivieren, nachdem Sie bestätigt haben, dass das `bncert` Tool auf Ihrer Instance installiert ist.

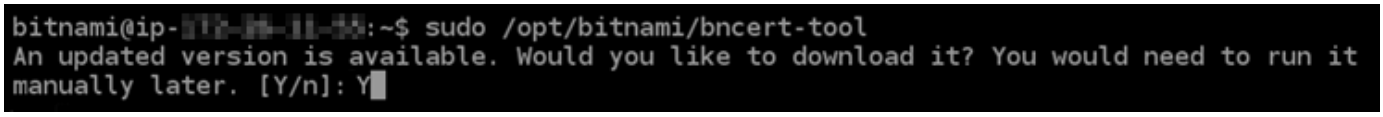
1. Geben Sie den folgenden Befehl ein, um das `bncert`-Tool auszuführen.

   ```
   sudo /opt/bitnami/bncert-tool
   ```

   Sie sollten eine Nachricht ähnlich dem folgenden Beispiel erhalten.

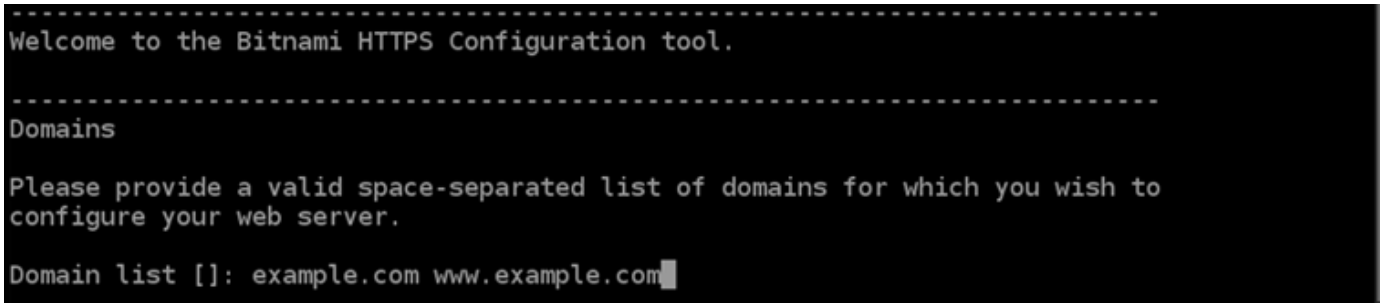
   

   Wenn das `bncert`-Tool eine Zeit lang auf Ihrer Instance installiert wurde, wird möglicherweise eine Meldung angezeigt, die angibt, dass eine aktualisierte Version des Tools verfügbar ist. Wählen Sie herunterladen, wie im folgenden Beispiel gezeigt, und geben Sie dann den`sudo /opt/bitnami/bncert-tool`-Befehl um das `bncert`-Tool nochmal auszuführen ein.

2. Geben Sie Ihren primären Domänennamen und alternative Domänennamen durch ein Leerzeichen getrennt ein, wie im folgenden Beispiel gezeigt.

   Wenn Ihre Domäne nicht darauf konfiguriert ist, Datenverkehr auf die öffentliche IP-Adresse Ihrer Instance umzuleitent, wird das`bncert`-Tool Sie aufgefordern, diese Konfiguration vorzunehmen, bevor Sie fortfahren. Ihre Domäne muss den Datenverkehr an die öffentliche IP-Adresse der Instance weiterleiten, von der Sie das `bncert`-Tool verwenden, um HTTPS für die Instance zu aktivieren. Dies bestätigt, dass Sie Eigentümer der Domäne sind und dient als Validierung für Ihr Zertifikat.



3. Das `bncert`-Tool wird Sie fragen, wie die Umleitung Ihrer Website konfiguriert werden soll. Die folgenden Optionen sind verfügbar:

   - Aktivieren einer Umleitung von HTTP zu HTTPS- Gibt an, ob Benutzer, die zur HTTP-Version Ihrer Website navigieren (d. h.`http://example.com`) automatisch auf die HTTPS-Version umgeleitet (d.h.`https://example.com`) werden. Wir empfehlen, diese Option zu aktivieren, da sie alle Besucher zwingt, die verschlüsselte Verbindung zu verwenden. `Y` eingeben und Eingabe drücken, um dies zu aktivieren.
   - Umleitung von Nicht-www zu www aktivieren- Gibt an, ob Benutzer, die zur Spitze Ihrer Domäne navigieren (d. h.`https://example.com`) automatisch an die`www`Unterdomäne Ihrer Domäne (d. h.`https://www.example.com`) weitergeleitet werden. Wir empfehlen, diese Option zu auszuwählen. Sie können diese jedoch deaktivieren und die alternative Option aktivieren (aktivieren Sie`www` auf Nicht-`www` Umleiten), wenn Sie die Spitze Ihrer Domäne als bevorzugte Website-Adresse in Suchmaschinentools wie den Webmaster-Tools von Google angegeben haben, oder wenn Ihre Spitze direkt auf Ihre IP verweist und Ihre `www` Unterdomäne Ihren Apex über eine CNAME-Akte referenziert. `Y` eingeben und Eingabe drücken, um dies zu aktivieren.
   - Umleitung von Nicht-www zu www aktivieren- Gibt an, ob Benutzer, die zur Unterdomäne Ihrer Domäne `www` navigieren (d. h.`https://www.example.com`) automatisch an die Spitze Ihrer Domäne (d. h.`https://example.com`) weitergeleitet werden. Wir empfehlen dies zu deaktivieren, wenn Sie Nicht-`www`Umleiten auf`www` aktiviert haben. `N` eingeben und Eingabe drücken, um dies zu aktivieren.

   Ihre Auswahl sollte wie im folgenden Beispiel aussehen.

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.



Enable HTTP to HTTPS redirection [Y/n]: Y



Enable non-www to www redirection [Y/n]: Y



Enable www to non-www redirection [y/N]: N
```

4. Die Änderungen, die vorgenommen werden, sind aufgelistet. Y eingeben undEingabe drücken, um zu bestätigen und fortzufahren.

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
 www.example.com)
7. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

5. Geben Sie Ihre E-Mail-Adresse ein, die Sie Ihrem Let's-Encrypt-Zertifikat zuordnen möchten, und drücken SieEingabe.

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

6. Lesen Sie die Let's-Encrypt-Subscriber-Vereinbarung. Y eingeben undEingabe drücken, um die Vereinbarung zu akzeptieren und fortzufahren.

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

Die Aktionen werden ausgeführt, um HTTPS für Ihre Instance zu aktivieren, einschließlich der Anforderung des Zertifikats und der Konfiguration der angegebenen Umleitungen.

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.
```

Ihr Zertifikat wurde erfolgreich ausgestellt und validiert, und die Umleitungen werden erfolgreich für Ihre Instance konfiguriert, wenn eine Meldung ähnlich dem folgenden Beispiel angezeigt wird.

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:
```

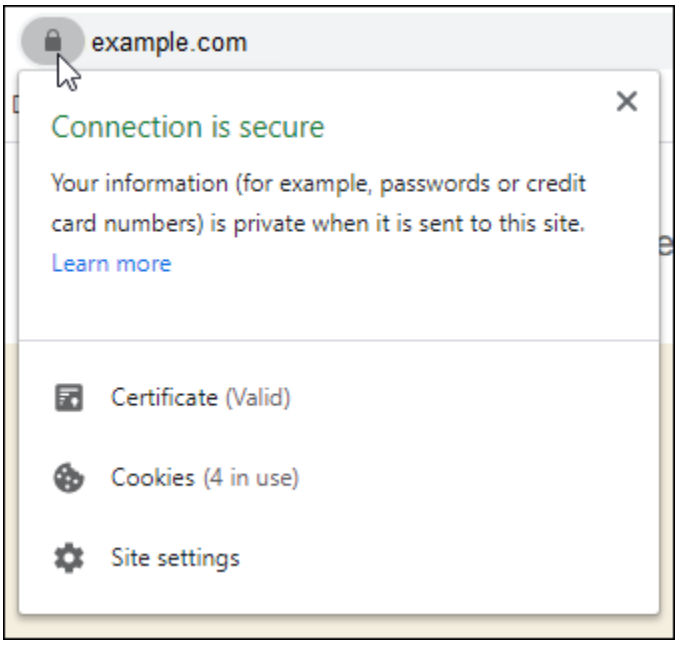
Das `bncert`-Tool führt alle 80 Tage vor Ablauf Ihres Zertifikats eine automatische Erneuerung durch. Wiederholen Sie die obigen Schritte, wenn Sie zusätzliche Domänen und Unterdomänen mit Ihrer Instance verwenden möchten und Sie HTTPS für diese Domänen aktivieren möchten.

Sie sind jetzt mit der Aktivierung von HTTPS auf Ihrer WordPress Instance fertig. Fahren Sie mit dem AbschnittSchritt 6: Prüfen, ob Ihre der Website HTTPS verwendetin diesem Leitfaden fort.

Schritt 6: Prüfen, ob Ihre Website HTTPS verwendet

Nachdem Sie HTTPS auf Ihrer WordPress Instance aktiviert haben, sollten Sie überprüfen, ob Ihre Website HTTPS verwendet, indem Sie alle Domains aufrufen, die Sie bei der Verwendung des `bncert` Tools angegeben haben. Wenn Sie jede Domäne besuchen, sollten Sie sehen, dass sie eine sichere Verbindung verwenden, wie im folgenden Beispiel gezeigt.

> **Note**
>
> Möglicherweise müssen Sie den Cache Ihres Browsers aktualisieren und bereinigen, um die Änderung zu sehen.



Sie könnten auch feststellen, dass die nicht-`www`-Adresse an die`www` Unterdomäne Ihrer Domäne oder umgekehrt umleitet, abhängig von der Option, die Sie beim Ausführen des`bncert`--Tools ausgewählt haben.

Migrieren eines vorhandenen WordPress Blogs zu Amazon Lightsail

Möchten Sie Ihren WordPress Hosting-Anbieter ändern? Amazon Lightsail ist der einfachste Weg, eine WordPress Website auf auszuführenAWS.

Sie können eines unserer Preismodelle wählen (ab 3,50 USD pro Monat) und haben die volle Kontrolle über Ihre WordPress Installation, einschließlich Plug-Ins, Designs und mehr.

Das Erstellen einer Lightsail- WordPress Instance dauert nur wenige Minuten. Folgen Sie diesem Tutorial, um Ihren vorhandenen WordPress Blog zu sichern und in eine neue Instance zu importieren, die in Lightsail ausgeführt wird.

Es folgt eine kurze Übersicht über den Prozess:

Lesen Sie weiter, um loszulegen.

Voraussetzungen

Bevor Sie beginnen, muss Folgendes sichergestellt sein:

1. Sie benötigen ein AWS-Konto. Registrieren Sie sich bei AWS oder melden Sie sich bei AWS an, wenn Sie bereits ein Konto haben.
2. Stellen Sie sicher, dass Ihr Konto für die Verwendung von Lightsail eingerichtet ist. Wenn Sie Ihr Konto vor längerer Zeit erstellt haben, oder wenn Sie noch keine Kreditkarte bereitgestellt haben, müssen Sie sich möglicherweise zuerst bei der AWS Management Console anmelden und Ihr Konto aktualisieren.

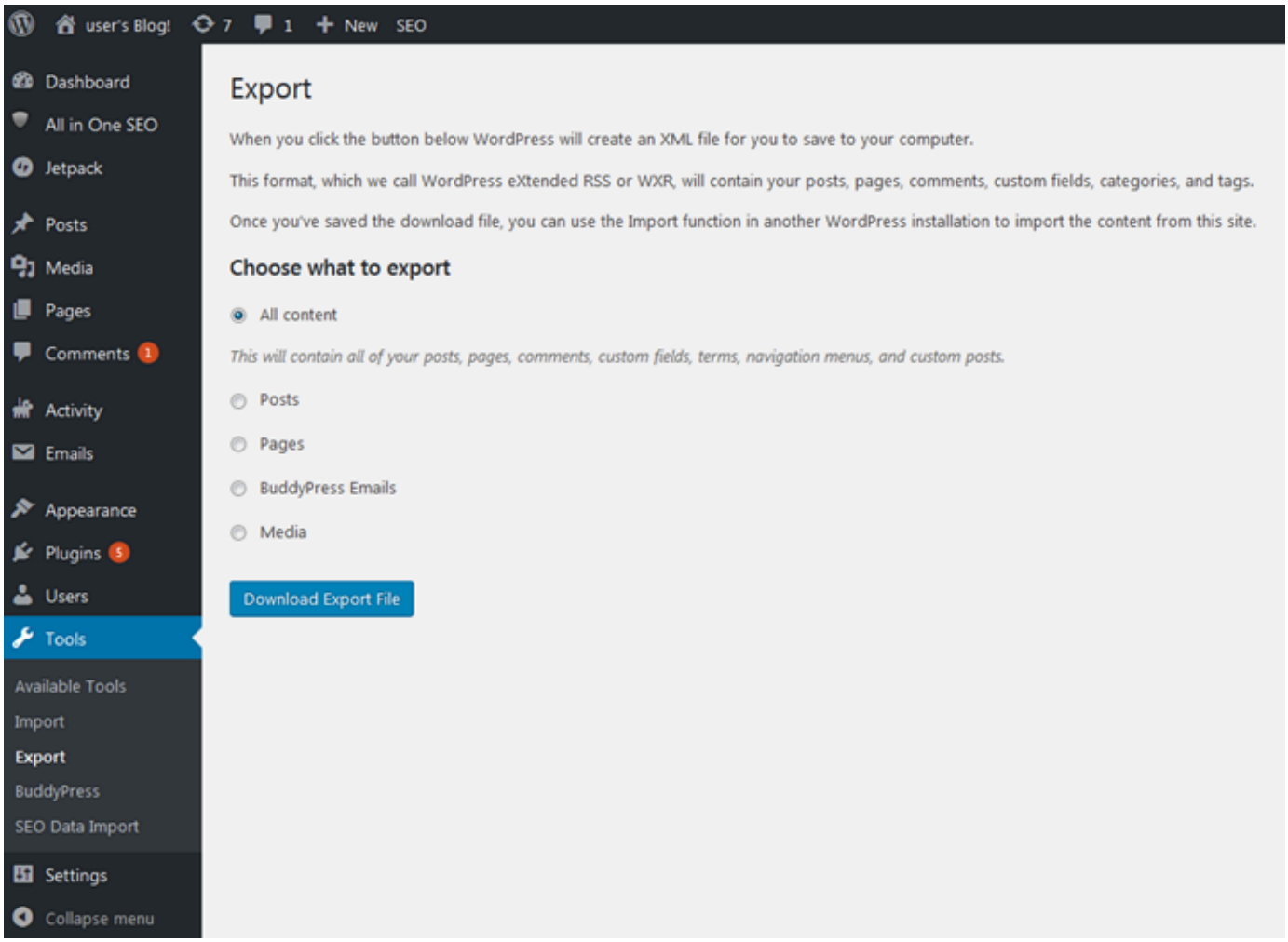
Schritt 1: Sichern Ihres vorhandenen WordPress Blogs

Sie können verwenden WordPress , um Ihren vorhandenen Blog zu sichern. Sie müssen sich nur bei der WordPress Admin-Konsole anmelden und Ihren Blog verwalten können.

1. Gehen Sie in Ihren Blog und wählen Sie Manage (Verwalten) aus.

   Wenn das Banner Manage (Verwalten) nicht angezeigt wird, können Sie die Anmeldeseite erreichen, indem Sie zu `http://<PublicIP>/wp-login.php` gehen. Ersetzen Sie `<PublicIP>` durch die öffentliche IP-Adresse Ihrer Instance.

2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein, um sich bei der WordPress Admin-Konsole anzumelden.
3. Wählen Sie im WordPress Dashboard Tools und dann Exportieren aus.
4. Wählen Sie auf der Seite Export (Exportieren) All content (Alle Inhalte), um alles als XML-Datei zu exportieren.



5. Wählen Sie Download export file (Export-Datei herunterladen), um Ihren alten Blog als XML-Datei herunterzuladen.

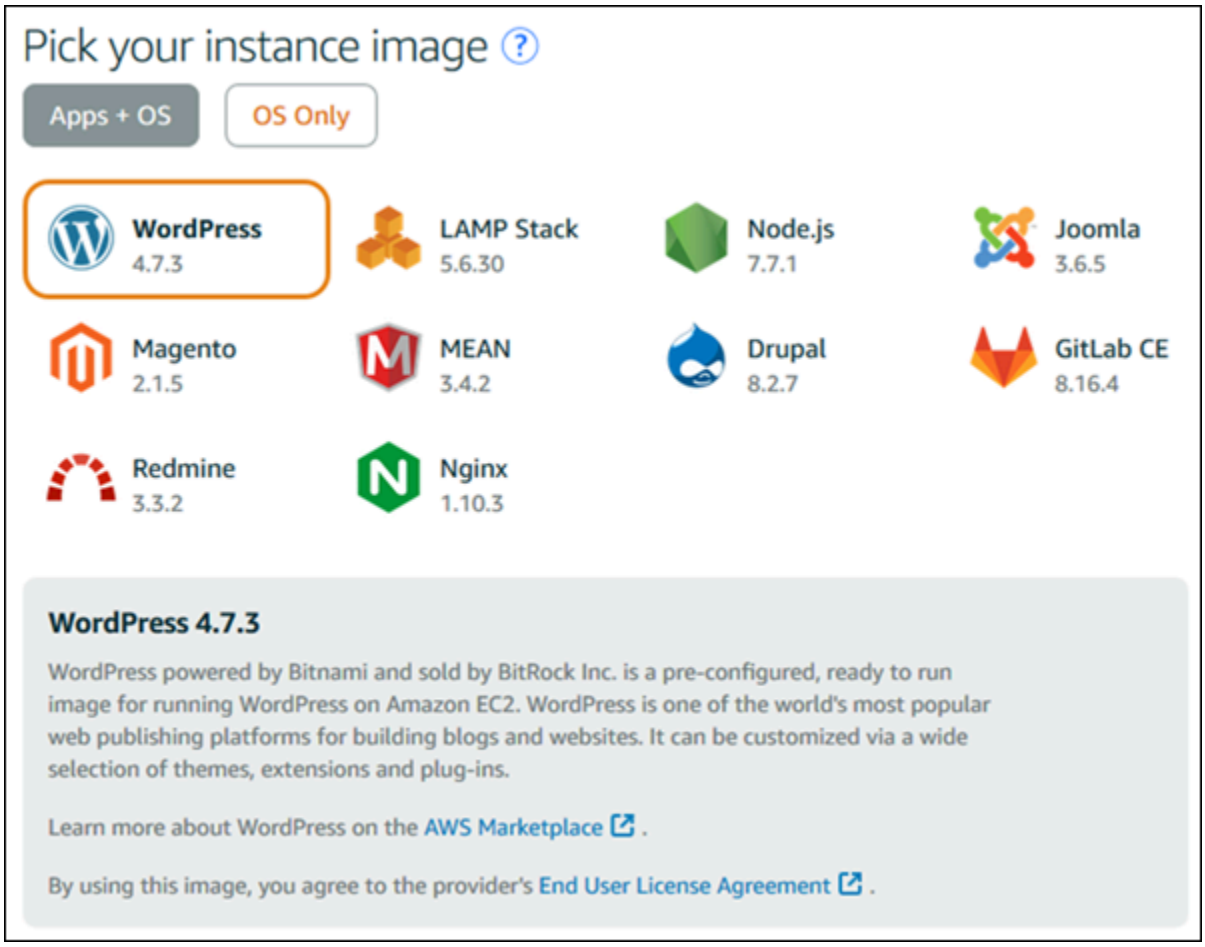
   Speichern Sie die XML-Datei an einem Standort, der einfach zu finden ist. Sie brauche sie in Schritt 4.

Schritt 2: Erstellen einer neuen WordPress Instance in Lightsail

Sie können in Lightsail in nur wenigen Minuten eine neue WordPress Instance erstellen. Das geht so:

1. Gehen Sie zur Lightsail-Startseite und melden Sie sich an.
2. Wählen Sie Create instance (Instance erstellen).
3. Wählen Sie die AWS-Region, in der Sie Ihren Blog erstellen möchten.

   Sie können die standardmäßige Availability Zone auswählen oder diese ändern, sobald Sie eine AWS-Region ausgewählt haben.
4. Wählen Sie WordPress.



5. Wählen Sie Ihren Instance-Plan (oder das Paket).

   Sie können Ihren Lightsail-Plan bei Bedarf später aktualisieren. Weitere Informationen finden Sie unter Erstellen einer Instance aus einem Snapshot in Lightsail.
6. Geben Sie einen Namen für Ihre Instance ein.

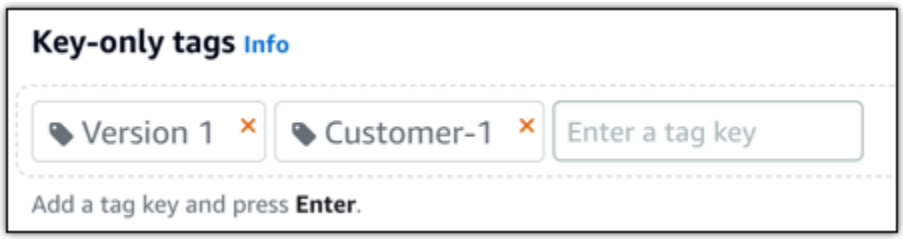
   Ressourcennamen:

   - Muss in jedem AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss 2–255 Zeichen enthalten.

- Muss mit einem alphanumerischen Zeichen beginnen und enden.
- Kann alphanumerische Zeichen, Punkte, Bindestriche und Unterstriche enthalten.

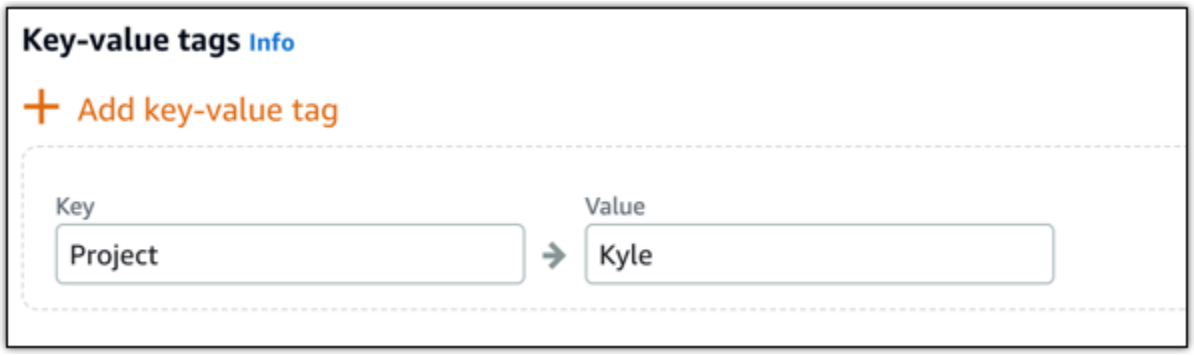
7. Wählen Sie eine der folgenden Optionen, um Ihrer Instance Tags hinzuzufügen:

   - Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.

   - Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

     Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.

   > **Note**
   >
   > Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

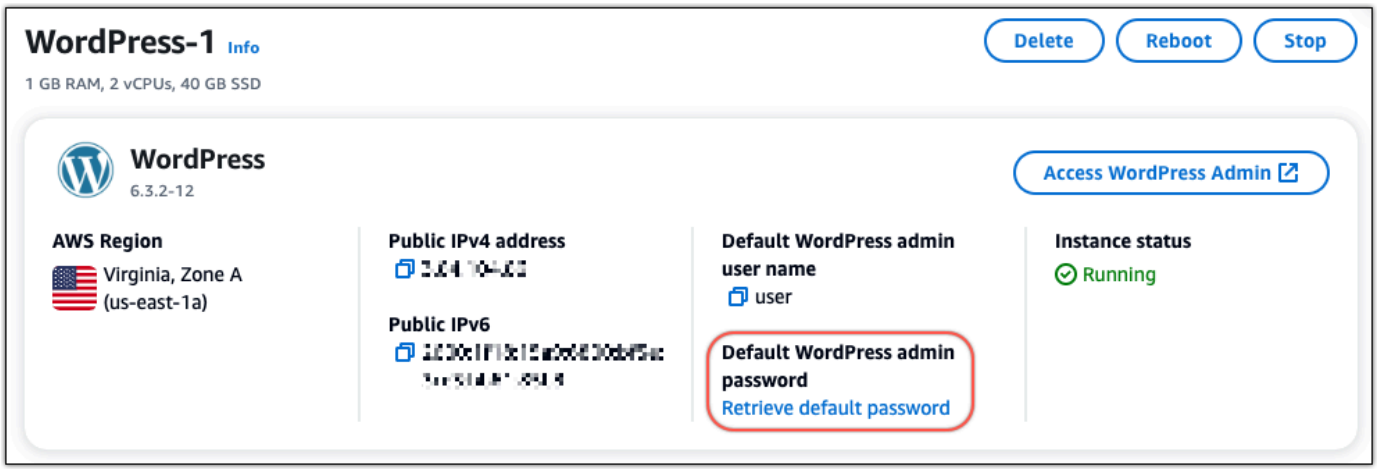
8. Wählen Sie Create instance (Instance erstellen).

Schritt 3: Melden Sie sich bei Ihrem neuen Lightsail- WordPress Blog an

Nachdem Sie nun einen neuen Blog in Lightsail haben, müssen Sie auf das WordPress Dashboard zugreifen, um Ihre alten Blogdaten zu importieren. Das Standardpasswort für die Anmeldung beim Verwaltungs-Dashboard Ihrer WordPress Website wird auf der Instance gespeichert. Führen Sie die folgenden Schritte aus, um das Passwort zu erhalten.

So rufen Sie das Standardpasswort für den WordPress Administrator ab

1. Öffnen Sie die Instance-Verwaltungsseite für Ihre WordPress Instance.
2. Wählen Sie im WordPress Bereich Standardpasswort abrufen aus. Dadurch wird unten auf der Seite das Standardpasswort für den Zugriff erweitert.



3. Wählen Sie Launch aus CloudShell. Dadurch wird unten auf der Seite ein Bereich geöffnet.
4. Wählen Sie Kopieren und fügen Sie dann den Inhalt in das CloudShell Fenster ein. Sie können entweder den Cursor an der CloudShell Eingabeaufforderung platzieren und Strg+V drücken, oder Sie können mit der rechten Maustaste klicken, um das Menü zu öffnen, und dann Einfügen wählen.
5. Notieren Sie sich das im CloudShell Fenster angezeigte Passwort. Sie benötigen dies, um sich beim Verwaltungs-Dashboard Ihrer WordPress Website anzumelden.

```
[cloudshell-user@ip-[redacted] ~]$ AWS_REGION=us-east-1 ~/lightsail_connect WordPress-1 cat bitnami_applic
ation_password
JKzh8wB5FAR!
```

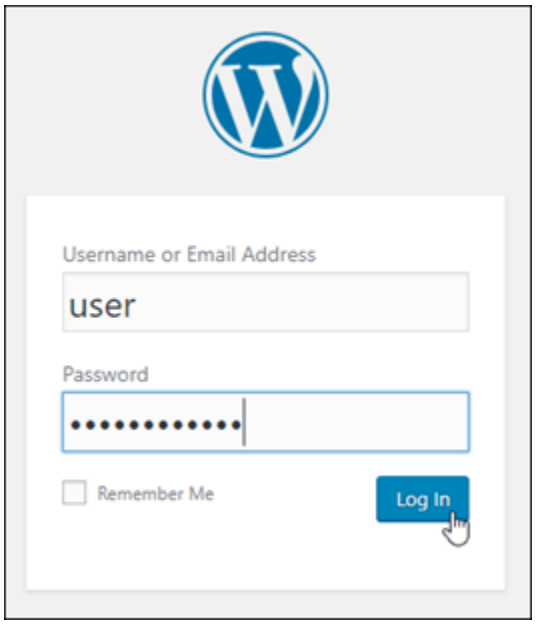
Nachdem Sie nun das Passwort für das Verwaltungs-Dashboard Ihrer WordPress Website haben, können Sie sich anmelden. Im Verwaltungs-Dashboard können Sie Ihr Benutzerpasswort ändern, Plugins installieren, das Design Ihrer Website ändern und vieles mehr.

Führen Sie die folgenden Schritte aus, um sich beim Verwaltungs-Dashboard Ihrer WordPress Website anzumelden.

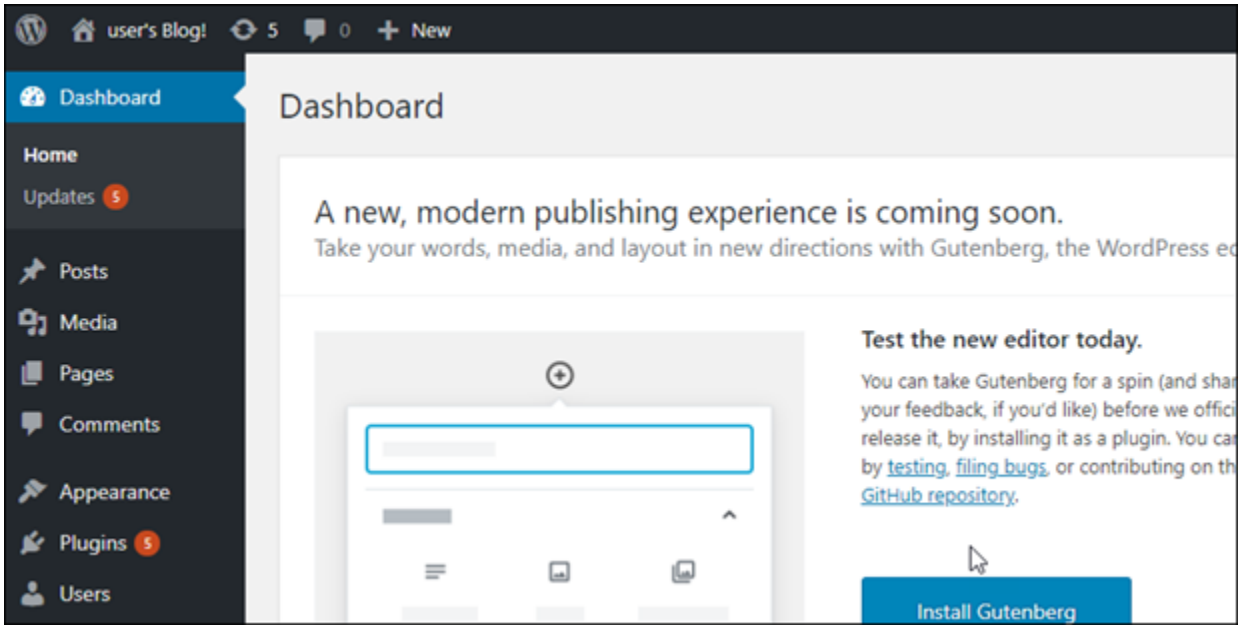
So melden Sie sich beim Verwaltungs-Dashboard an

1. Öffnen Sie die Instance-Verwaltungsseite für Ihre WordPress Instance.
2. Wählen Sie im WordPress Bereich Access WordPress Admin aus.
3. Wählen Sie im Bereich Zugriff auf Ihr WordPress Admin-Dashboard unter Öffentliche IP-Adresse verwenden den Link mit diesem Format aus:

   http://*public-ipv4-address* ./wp-admin
4. Geben Sie für Benutzername oder E-Mail-Adresse ein**`user`**.
5. Geben Sie für Passwort das im vorherigen Schritt erhaltene Passwort ein.
6. Wählen Sie Log in (Anmelden).



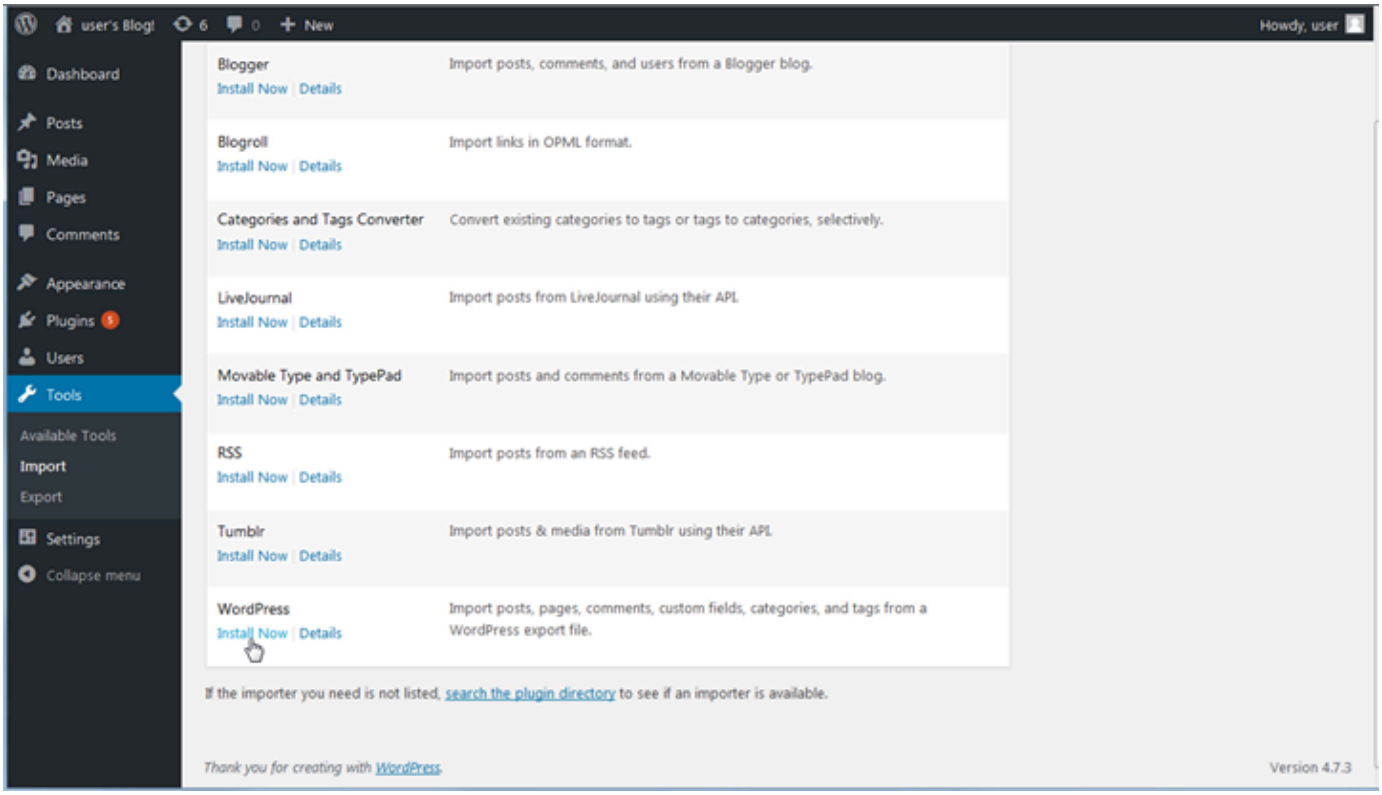
Sie sind jetzt beim Verwaltungs-Dashboard Ihrer WordPress Website angemeldet, auf dem Sie administrative Aktionen ausführen können. Weitere Informationen zur Verwaltung Ihrer WordPress Website finden Sie unter WordPress Codex in der - WordPress Dokumentation.



Schritt 4: Importieren Ihrer XML-Datei in Ihren neuen Lightsail-Blog

Sobald Sie sich erfolgreich beim WordPress Dashboard auf Ihrer neuen Lightsail-Instance angemeldet haben, führen Sie die folgenden Schritte aus, um die XML-Datei in Ihren neuen Lightsail-Blog zu importieren.

1. Wählen Sie im WordPress Dashboard Ihrer neuen Lightsail-Instance Tools aus.
2. Wählen Sie Importieren und dann Jetzt installieren, um das WordPress Import-Tool zu installieren.



3. Sobald das Tool installiert ist, wählen Sie Run Importer (Importer ausführen), um das Import-Tool auszuführen.
4. Wählen Sie auf der Seite Import WordPress die Option Durchsuchen aus.
5. Suchen Sie die XML-Datei, die Sie in Schritt 1: Sichern Ihres vorhandenen WordPress Blogs gespeichert haben, und wählen Sie dann Öffnen aus.
6. Wählen Sie Upload file and import (Datei hochladen und importieren).

   Akzeptieren Sie die restlichen Standardeinstellungen, und klicken Sie dann auf Submit (Senden).

Nächste Schritte

Sie können überprüfen, ob alles funktioniert hat, indem Sie Ihren Blog (neben dem Home-Symbol) und dann im WordPress Dashboard die Option Website besuchen auswählen. Sie können auch die IP-Adresse in einen Browser eingeben und den Blog anzeigen.

Hier einige nächste Schritte:

- Migrieren Sie Ihren DNS, sodass Ihre Domänen-Nameserver auf die neue Version Ihres Blogs verweisen.

- Passen Sie das Erscheinungsbild Ihres neuen Blogs an und/oder installieren Sie einige WordPress Plugins.
- HTTPS-Support mit SSL-Zertifikaten aktivieren

WordPress-Multisite-Tutorials für Amazon Lightsail

WordPress Multisite ermöglicht es Administratoren, mehrere Websites von derselben WordPress-Instance aus zu hosten und zu verwalten. In den folgenden Tutorials erfahren Sie, wie Sie mit WordPress Multisite in Lightsail arbeiten.

Themen

- Blogs als Domänen zu Ihrer WordPress Multisite-Instance in Lightsail hinzufügen
- Blogs als Subdomänen zu Ihrer WordPress Multisite-Instance in Lightsail hinzufügen
- Definieren der primären Domäne für Ihre WordPress Multisite-Instance in Lightsail

Blogs als Domänen zu Ihrer WordPress Multisite-Instance in Lightsail hinzufügen

Eine WordPress Multisite-Instance in Amazon Lightsail ist so konzipiert, dass sie mehrere Domänen oder Subdomains für jede Blog-Site verwendet, die Sie innerhalb dieser Instance erstellen. In diesem Leitfaden zeigen wir Ihnen, wie Sie eine Blog-Site mit einer anderen Domäne als der primären Domäne Ihres Hauptblogs auf Ihrer WordPress Multisite-Instance hinzufügen können. Wenn beispielsweise die primäre Domäne Ihres Hauptblogs `example.com` ist, können Sie neue Blog-Sites erstellen, die die Domänen `another-example.com` und `third-example.com` auf derselben Instance verwenden.

> **Note**
>
> Sie können außerdem Sites mit Subdomänen zu Ihrer WordPress Multisite-Instance hinzufügen. Weitere Informationen finden Sie unter Hinzufügen von Blogs als Subdomains zu Ihrer WordPress-Multisite-Instance.

Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen in der angezeigten Reihenfolge:

1. Erstellen Sie eine WordPress Multisite-Instance in Lightsail. Weitere Informationen finden Sie unter Erstellen einer Instance.
2. Erstellen Sie eine statische IP und hängen Sie sie an Ihre WordPress Multisite-Instance in Lightsail an. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.
3. Fügen Sie Ihre Domäne zu Lightsail hinzu, indem Sie eine DNS-Zone erstellen, und verweisen Sie für diese dann auf die statische IP, die Sie an Ihre WordPress Multisite-Instance angehängt haben. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.
4. Definieren der primären Domain für Ihre WordPress-Multisite-Instance. Weitere Informationen finden Sie unter Definieren der primären Domain für Ihre WordPress-Multisite-Instance.

Blog als Domäne zu Ihrer WordPress Multisite-Instance hinzufügen

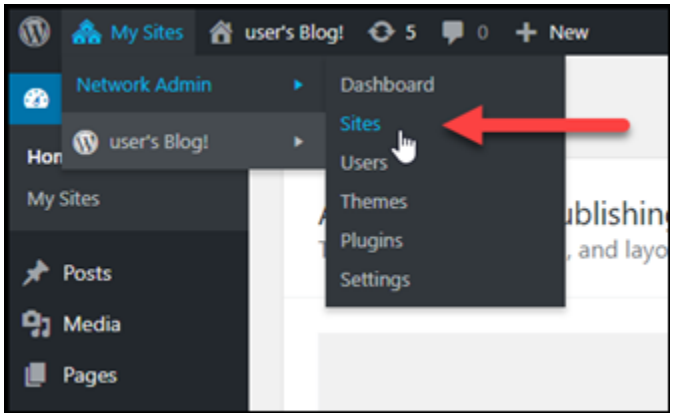
Führen Sie diese Schritte aus, um eine Blog-Site in Ihrer WordPress Multisite-Instance zu erstellen, die eine andere Domäne verwendet als die primäre Domäne Ihres Hauptblogs.

> **Important**
>
> Bevor Sie diese Schritte ausführen, müssen Sie Schritt 4 ausführen, der im Abschnitt zu den Voraussetzungen dieses Leitfadens aufgeführt ist.

1. Melden Sie sich im Dashboard der Administration Ihrer WordPress Multisite-Instance an.

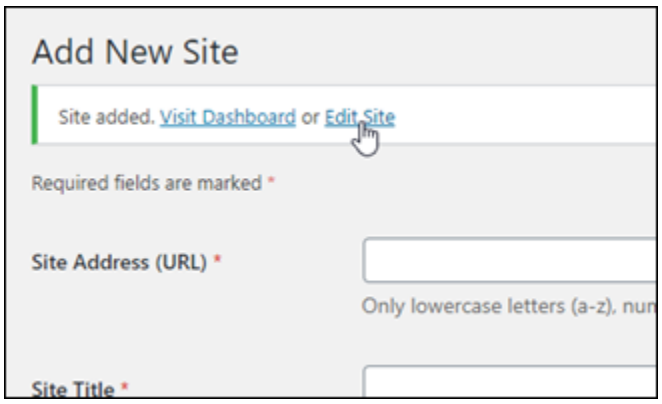
   > **Note**
   >
   > Weitere Informationen finden Sie unter Abrufen des Anwendungs-Benutzernamens und des Passworts für Ihre Bitnami-Instance.

2. Wählen Sie My Sites (Meine Sites), Network Admin (Netzwerkadmin) und Sites im oberen Navigationsbereich aus.

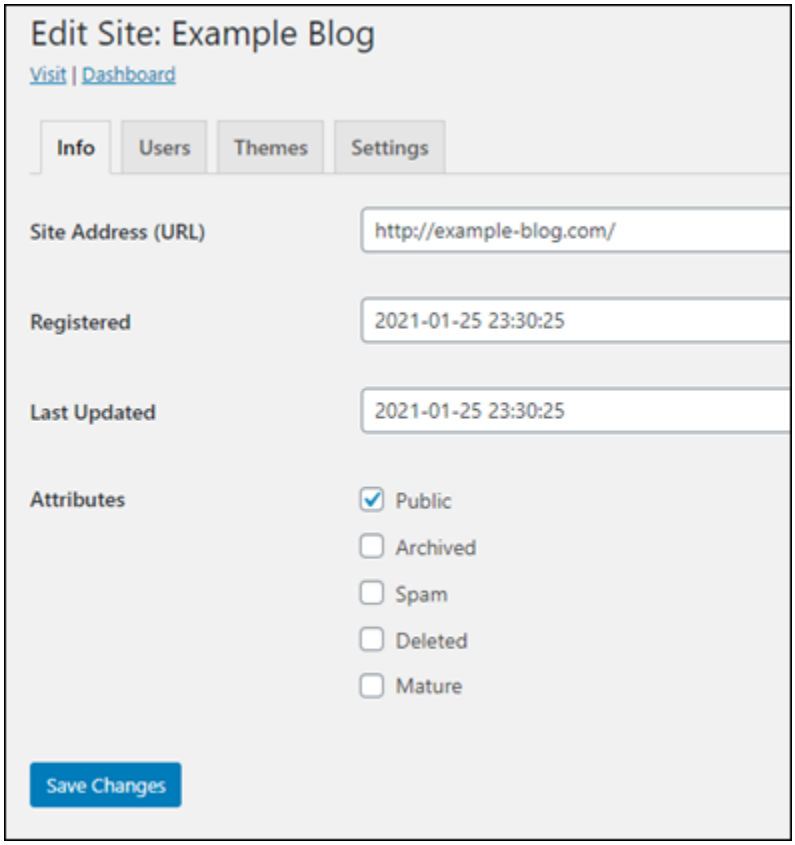


3. Wählen Sie Add New (Neue hinzufügen) aus, um eine neue Blog-Site hinzuzufügen.
4. Geben Sie eine Standortadresse im Textfeld Site-Adresse (URL) ein. Dies ist eine Domäne, die für die neue Blog-Site verwendet wird. Wenn Ihre neue Blog-Seite beispielsweise `example-blog.com` als Domäne verwendet, geben Sie `example-blog` in das Textfeld Seiten-Adresse (URL) ein. Ignorieren Sie das auf der Seite angezeigte primäre Domänensuffix.

5. Geben Sie einen Seitentitel ein, wählen Sie eine Seitensprache aus und geben Sie eine Admin-E-Mail-Adresse ein.
6. Wählen Sie Add Site (Site hinzufügen) aus.
7. Wählen Sie Seite bearbeiten im Bestätigungsbanner aus, das auf der Seite erscheint. Dadurch werden Sie umgeleitet, um die Details der Website zu bearbeiten, die Sie kürzlich erstellt haben.

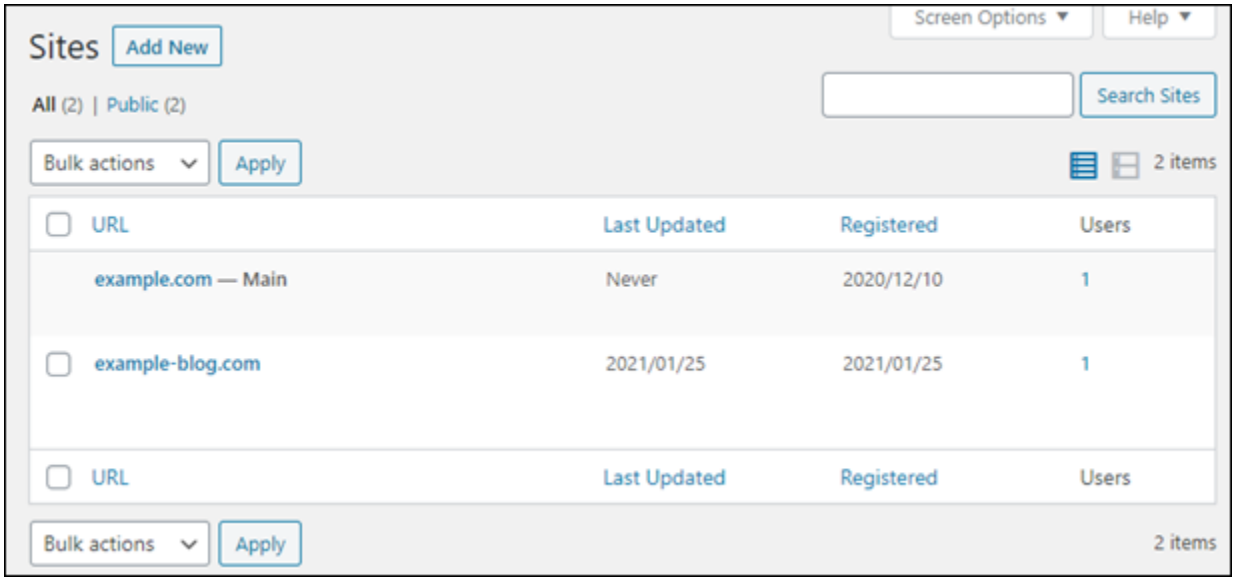


8. Ändern Sie auf der Seite Seite bearbeiten die im Textfeld Seiten-Adresse (URL) aufgeführte Unterdomäne in die Apex-Domäne, die Sie verwenden möchten. In diesem Beispiel haben wir `http://example-blog.com` angegeben.



9. Wählen Sie Save Changes.

   Jetzt wurde die neue Blog-Site in Ihrer WordPress Multisite-Instance erstellt, aber die Domäne noch nicht für die Weiterleitung zur neuen Blog-Site konfiguriert. Fahren Sie mit dem nächsten Schritt fort, um einen Address-Datensatz (A-Datensatz) zur DNS-Zone Ihrer Domäne hinzuzufügen.



Address-Datensatz (A-Datensatz) zur DNS-Zone Ihrer Domäne hinzufügen

Führen Sie diese Schritte aus, um die Domäne für Ihre neue Blog-Site auf Ihre WordPress Multisite-Instance zu verweisen. Sie müssen diese Schritte für jede Blog-Site ausführen, die Sie auf Ihrer WordPress Multisite-Instance erstellen.

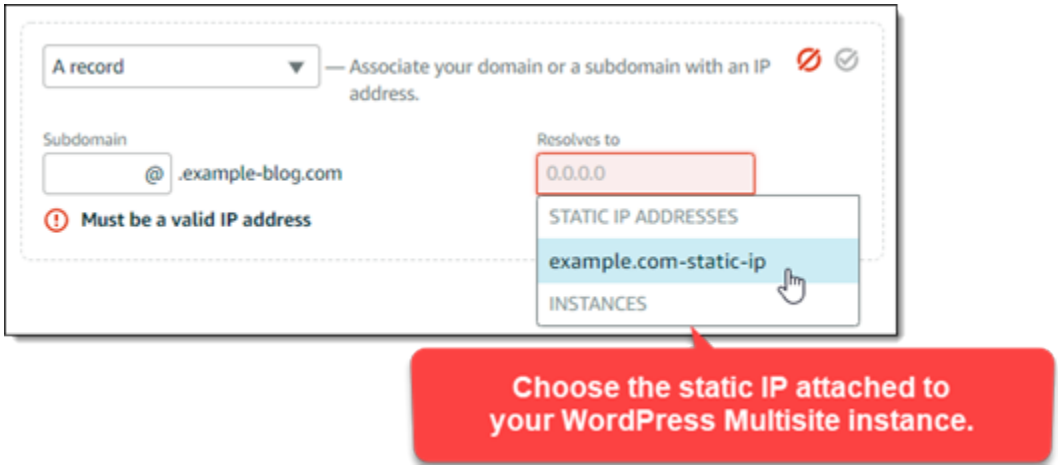
Zu Demonstrationszwecken verwenden wir die DNS-Zone von Lightsail. Die Schritte können jedoch für andere DNS-Zonen ähnlich sein, die typischerweise von Domänenvergabestellen gehostet werden.

> **Important**
>
> In der Lightsail-Konsole können Sie maximal sechs DNS-Zonen erstellen. Wenn Sie mehr DNS-Zonen benötigen, empfehlen wir Ihnen, Amazon Route 53 zur Verwaltung der DNS-Einträge Ihrer Domäne zu verwenden. Weitere Informationen finden Sie unter Amazon Route 53 zum DNS-Service für eine vorhandene Domain machen.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Domains & DNS (Domänen und DNS).
3. Wählen Sie unter dem Abschnitt DNS zones (DNS-Zonen) auf der Seite die DNS-Zone für die Domäne Ihrer neuen Blog-Site aus.

4. Wählen Sie im DNS-Zoneneditor die Registerkarte DNS records (DNS-Datensätze). Wählen Sie dann Add record (Datensatz hinzufügen) aus.

5. Wählen Sie A record (A-Datensatz) im Dropdown-Menü für die Datensatzart aus.
6. Geben Sie im Textfeld Record name (Datensatzname) ein "at"-Symbol (@) ein, um einen Datensatz für den Stamm der Domäne zu erstellen.
7. Wählen Sie im Textfeld Resolves to (Auflösung zu) die statische IP-Adresse aus, die an Ihre WordPress Multisite-Instance angehängt ist.



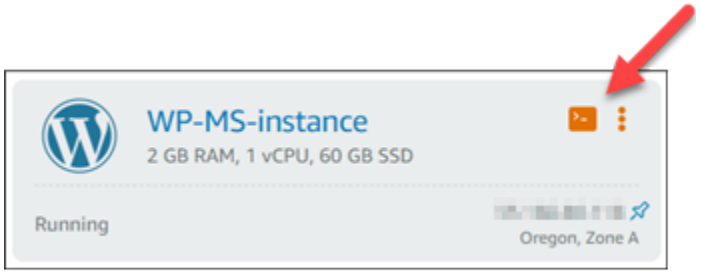
8. Wählen Sie Speichern.

   Nachdem sich die Änderung über das DNS des Internets verbreitet hat, leitet die Domäne den Datenverkehr an die neue Blog-Site auf Ihrer WordPress-Multisite-Instance weiter.

Aktivieren Sie die Cookie-Unterstützung, um die Anmeldung für Blog-Sites zu erlauben

Wenn Sie Blog-Sites als Domänen zu Ihrer WordPress-Multisite-Instance hinzufügen, müssen Sie auch die WordPress-Konfigurationsdatei (`wp-config`) auf Ihrer Instance aktualisieren, um die Cookie-Unterstützung zu aktivieren. Wenn Sie die Cookie-Unterstützung nicht aktivieren, kann es sein, dass Benutzer beim Versuch, sich beim WordPress-Administrations-Dashboard ihrer Blog-Sites anzumelden, den Fehler „Fehler: Cookies werden blockiert oder nicht unterstützt“ erhalten.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Klicken Sie auf der Lightsail-Startseite auf das SSH-Quick-Connect-Symbol für Ihre WordPress-Multisite-Instance.



3. Nachdem Ihre browserbasierte Lightsail-SSH-Sitzung verbunden ist, geben Sie den folgenden Befehl ein, um die `wp-config.php`-Datei auf Ihrer Instance mithilfe von Vim zu öffnen und zu ändern:

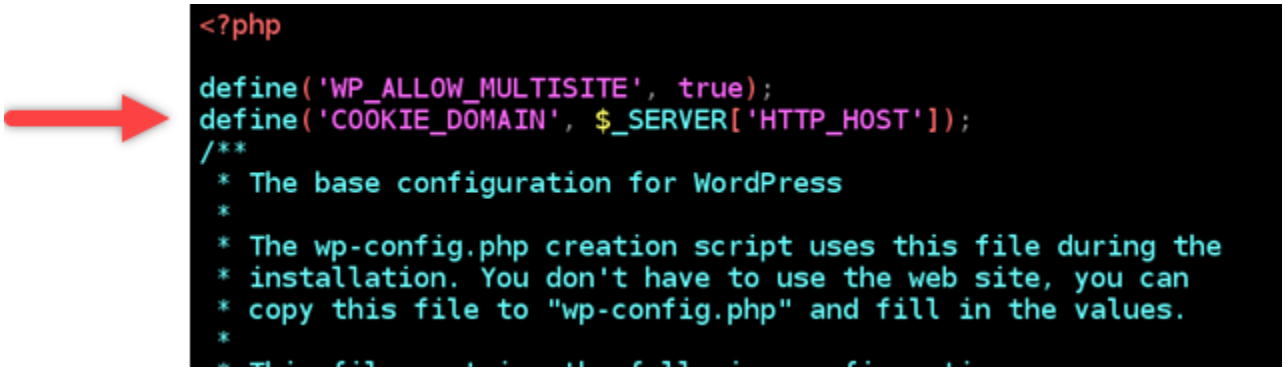
```
sudo vim /opt/bitnami/wordpress/wp-config.php
```

> **Note**
>
> Wenn dieser Befehl fehlschlägt, verwenden Sie möglicherweise eine ältere Version der WordPress-Multisite-Instance. Versuchen Sie, stattdessen den folgenden Befehl auszuführen.
>
> ```
> sudo vim /opt/bitnami/wordpress/wp-config.php
> ```

4. Drücken Sie I, um den Einfügemodus in Vim einzugeben.
5. Fügen Sie die folgende Textzeile unter der Textzeile `define('WP_ALLOW_MULTISITE', true);` hinzu.

```
define('COOKIE_DOMAIN', $_SERVER['HTTP_HOST']);
```

Wenn Sie fertig sind, sieht die Datei wie folgt aus:



6. Drücken Sie die Esc-Taste, um den Einfügemodus in Vim zu verlassen, geben Sie dann `:wq!` ein und drücken Sie die Enter-Taste, um Ihre Änderungen zu speichern (schreiben) und Vim zu beenden.
7. Geben Sie den folgenden Befehl ein, um die zugrunde liegenden Dienste der WordPress-Instance neu zu starten.

   ```
   sudo /opt/bitnami/ctlscript.sh restart
   ```

   Cookies sollten jetzt auf Ihrer WordPress-Multisite-Instance aktiviert sein, und Benutzer, die versuchen, sich bei ihren Blog-Sites anzumelden, wird nicht der Fehler „Fehler: Cookies werden blockiert oder nicht unterstützt“ angezeigt.

Nächste Schritte

Nachdem Sie Blogs als Domänen zu Ihrer WordPress-Multisite-Instance hinzugefügt haben, empfehlen wir Ihnen, sich mit der WordPress-Multisite-Administration vertraut zu machen. Weitere Informationen finden Sie unter Multisite-Netzwerkverwaltung in der WordPress-Dokumentation.

Blogs als Subdomänen zu Ihrer WordPress Multisite-Instance in Lightsail hinzufügen

Eine WordPress Multisite-Instance in Amazon Lightsail ist so konzipiert, dass sie mehrere Domänen oder Subdomains für jede Blog-Site verwendet, die Sie innerhalb dieser Instance erstellen. In diesem Handbuch zeigen wir Ihnen, wie Sie eine Blog-Site als Subdomäne Ihrer WordPress Multisite-Instance hinzufügen können. Wenn beispielsweise die primäre Domäne Ihres Hauptblogs `example.com` ist, können Sie neue Blog-Sites erstellen, die die Subdomänen `earth.example.com` und `moon.example.com` auf derselben Instance verwenden.

> **Note**
>
> Sie können außerdem Sites mit Domänen zu Ihrer WordPress Multisite-Instance hinzufügen. Weitere Informationen finden Sie unter Hinzufügen von Blogs als Domains zu Ihrer WordPress-Multisite-Instance.

Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen in der angezeigten Reihenfolge:

1. Erstellen einer WordPress Multisite-Instance. Weitere Informationen finden Sie unter Erstellen einer Instance.
2. Erstellen einer statischen IP und sie an Ihre WordPress Multisite-Instance anhängen. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.
3. Fügen Sie Ihre Domäne zu Lightsail hinzu, indem Sie eine DNS-Zone erstellen, und verweisen Sie für diese dann auf die statische IP, die Sie an Ihre WordPress Multisite-Instance angehängt haben. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.
4. Definieren der primären Domain für Ihre WordPress-Multisite-Instance. Weitere Informationen finden Sie unter Definieren der primären Domain für Ihre WordPress-Multisite-Instance.

Blog als Subdomäne zu Ihrer WordPress Multisite-Instance hinzufügen

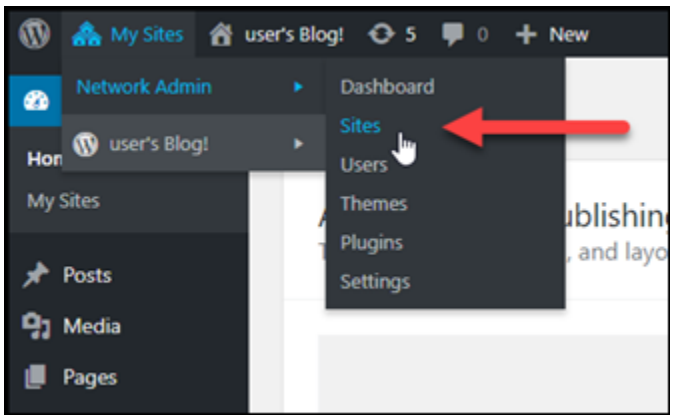
Führen Sie diese Schritte aus, um neue Blogs in Ihrer WordPress Multisite-Instance zu erstellen, die eine andere Subdomäne ihrer primären Domäne Ihres Hauptblogs verwenden.

> **Important**
>
> Bevor Sie diese Schritte ausführen, müssen Sie Schritt 4 ausführen, der im Abschnitt zu den Voraussetzungen dieses Leitfadens aufgeführt ist.

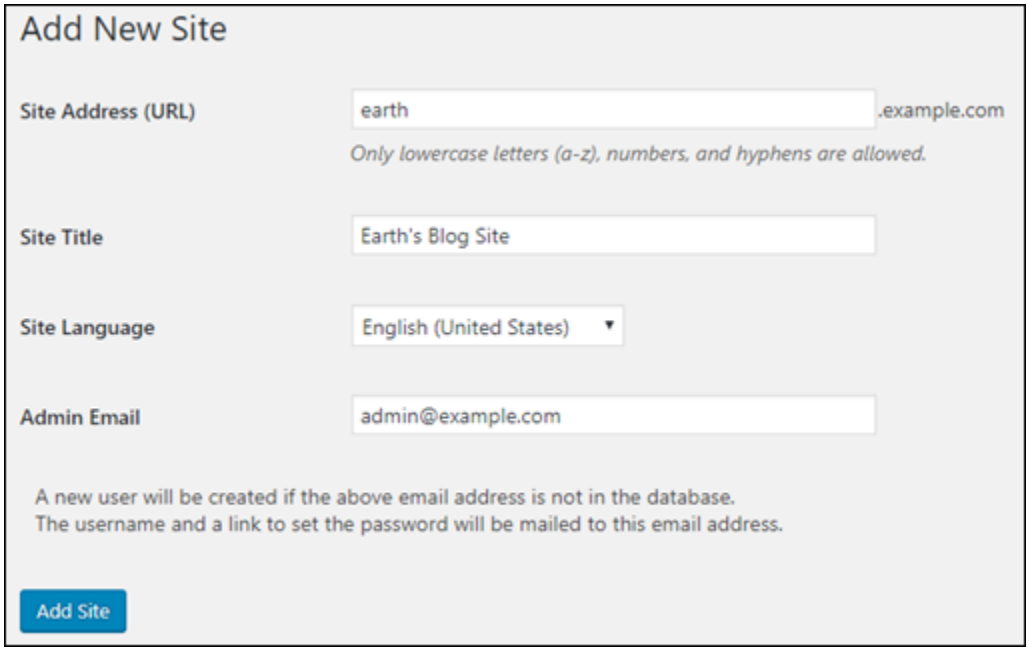
1. Melden Sie sich im Dashboard der Administration Ihrer WordPress Multisite-Instance an.

> **Note**
>
> Weitere Informationen finden Sie unter Abrufen des Anwendungs-Benutzernamens und des Passworts für Ihre Bitnami-Instance.

2. Wählen Sie My Sites (Meine Sites), Network Admin (Netzwerkadmin) und Sites im oberen Navigationsbereich aus.



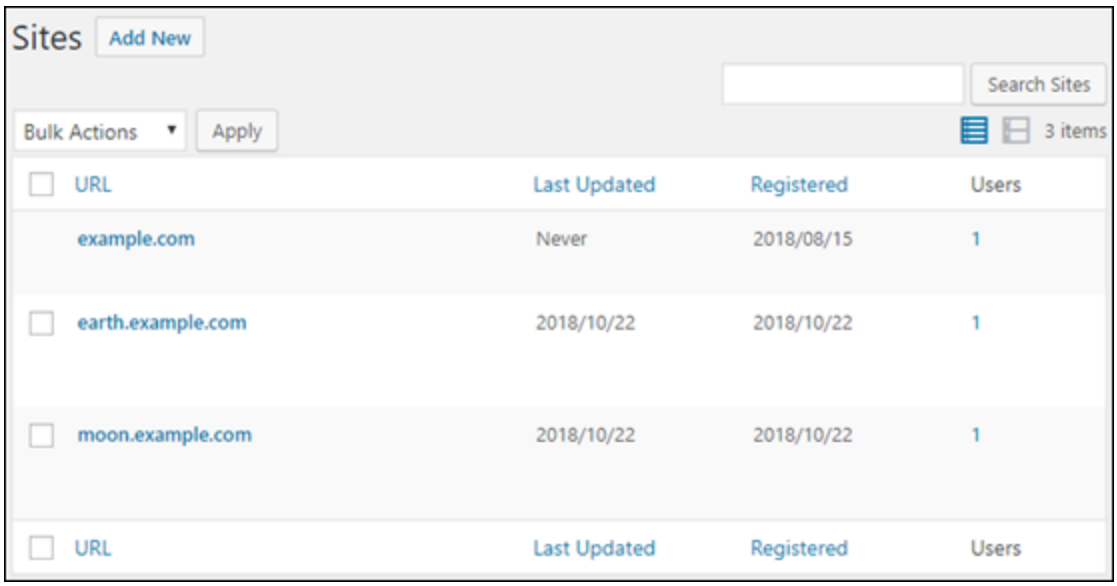
3. Wählen Sie Add New (Neue hinzufügen) aus, um eine neue Blog-Site hinzuzufügen.
4. Geben Sie eine Site-Adresse ein, die die Subdomäne ist, die für die neue Blog-Site verwendet wird.



5. Geben Sie einen Seitentitel ein, wählen Sie eine Seitensprache aus und geben Sie eine Admin-E-Mail-Adresse ein.

6. Wählen Sie Add Site (Site hinzufügen) aus.

   Jetzt wurde die neue Blog-Site in Ihrer WordPress Multisite-Instance erstellt, aber die Subdomäne noch nicht für die Weiterleitung zur neuen Blog-Site konfiguriert. Fahren Sie mit dem nächsten Schritt fort, um einen Address-Datensatz (A-Datensatz) zur DNS-Zone Ihrer Domäne hinzuzufügen.

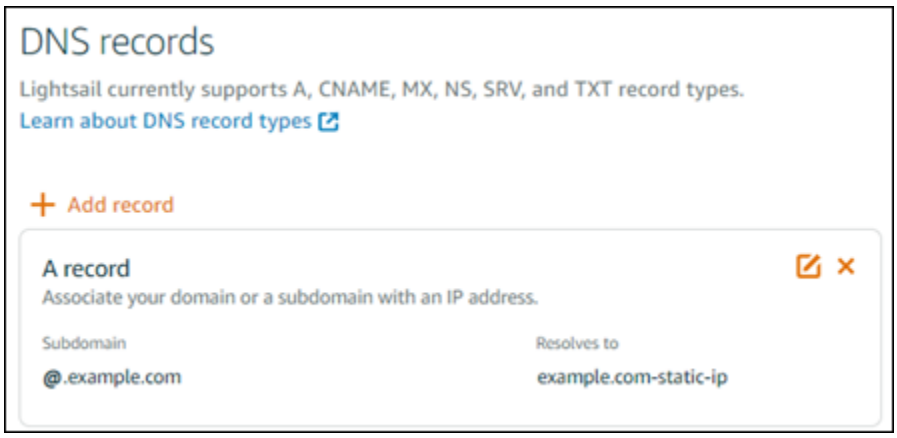


Address-Datensatz (A-Datensatz) zur DNS-Zone Ihrer Domäne hinzufügen

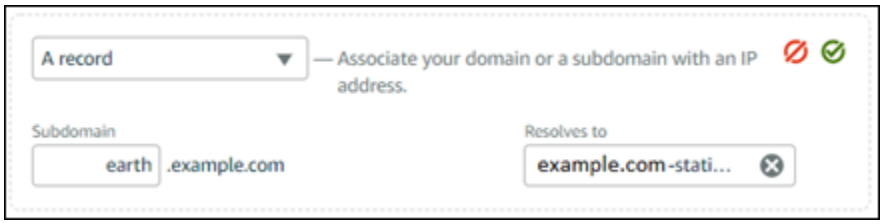
Führen Sie diese Schritte aus, um die Subdomäne für Ihre neue Blog-Site auf Ihre WordPress Multisite-Instance zu verweisen. Sie müssen diese Schritte für jede Blog-Site ausführen, die Sie auf Ihrer WordPress Multisite-Instance erstellen.

Zu Demonstrationszwecken verwenden wir die DNS-Zone von Lightsail. Die Schritte können jedoch für andere DNS-Zonen ähnlich sein, die typischerweise von Domänenvergabestellen gehostet werden.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Domains & DNS (Domänen und DNS).
3. Wählen Sie im Abschnitt DNS zones (DNS-Zonen) der Seite die DNS-Zone für die Domäne aus, die Sie als primäre Domäne für Ihre WordPress Multisite-Instance definiert haben.
4. Wählen Sie im DNS-Zoneneditor die Registerkarte DNS records (DNS-Datensätze). Wählen Sie dann Add record (Datensatz hinzufügen) aus.



5. Wählen Sie A record (A-Datensatz) im Dropdown-Menü für die Datensatzart aus.
6. Geben Sie im Textfeld Record name (Datensatzname) die Subdomäne ein, die Sie bei der Erstellung der neuen Blog-Website auf Ihrer WordPress Multisite-Instance als Website-Adresse festgelegt haben.
7. Wählen Sie im Textfeld Resolves to (Auflösung zu) die statische IP-Adresse aus, die an Ihre WordPress Multisite-Instance angehängt ist.



8. Wählen Sie Speichern.

   Das ist alles. Nachdem sich die Änderung über das DNS im Internet verbreitet hat, wird die Domäne auf die neue Blog-Site auf Ihrer WordPress Multisite-Instance umgeleitet.

Nächste Schritte

Nachdem Sie Blogs als Unterdomänen zu Ihrer WordPress-Multisite-Instance hinzugefügt haben, empfehlen wir Ihnen, sich mit der WordPress-Multisite-Administration vertraut zu machen. Weitere Informationen finden Sie unter Multisite-Netzwerkverwaltung in der WordPress-Dokumentation.

Definieren der primären Domäne für Ihre WordPress Multisite-Instance in Lightsail

Eine WordPress Multisite-Instance in Amazon Lightsail ist so konzipiert, dass sie mehrere Domänen oder Subdomains für jede Blog-Site verwendet, die Sie innerhalb dieser Instance erstellen. Aus

diesem Grund müssen Sie die primäre Domäne definieren, die für das Hauptblog Ihrer WordPress Multisite-Instance verwendet werden soll.

Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen in der angezeigten Reihenfolge:

1. Erstellen Sie eine WordPress Multisite-Instance in Lightsail. Weitere Informationen finden Sie unter Erstellen einer Instance.
2. Erstellen Sie eine statische IP und hängen Sie sie an Ihre WordPress Multisite-Instance in Lightsail an. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse und diese an eine Instance anfügen.

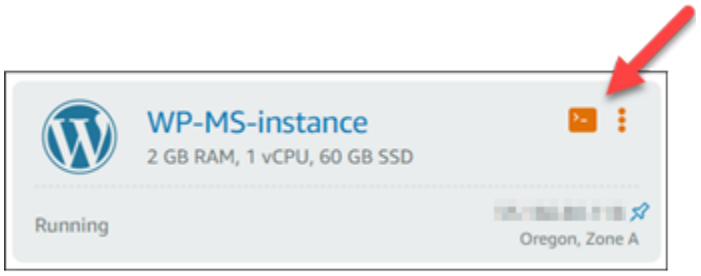
   > **Important**
   >
   > Sie müssen Ihre WordPress Multisite-Instance neu starten, nachdem Sie eine statische IP-Adresse hinzugefügt haben. Dies ermöglicht es der Instance, die damit verbundene neue statische IP zu erkennen.

3. Fügen Sie Ihre Domäne zu Lightsail hinzu, indem Sie eine DNS-Zone erstellen, und verweisen Sie für diese dann auf die statische IP, die Sie an Ihre WordPress Multisite-Instance angehängt haben. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.
4. Warten Sie einige Zeit, damit die DNS-Änderungen über das DNS im Internet verbreitet werden. Anschließend können Sie mit dem Abschnitt Definieren der primären Domäne für Ihre WordPress-Multisite-Instance in diesem Handbuch fortfahren.

Definieren der primären Domäne für Ihre WordPress Multisite-Instance

Führen Sie diese Schritte aus, um sicherzustellen, dass Ihre Domäne (z. B. `example.com`) zum Hauptblog Ihrer WordPress Multisite-Instance umgeleitet wird.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Klicken Sie auf der Lightsail-Startseite auf das SSH-Quick-Connect-Symbol für Ihre WordPress-Multisite-Instance.



3. Geben Sie den folgenden Befehl ein, um den primären Domänennamen für Ihre WordPress Multisite-Instance zu definieren. Achten Sie darauf, *<domain>* durch den richtigen Domänennamen für Ihre WordPress Multisite zu ersetzen.

```
sudo /opt/bitnami/configure_app_domain --domain <domain>
```

Beispiel:

```
sudo /opt/bitnami/configure_app_domain --domain example.com
```

> **Note**
>
> Wenn dieser Befehl fehlschlägt, verwenden Sie möglicherweise eine ältere Version der WordPress Multisite-Instance. Versuchen Sie stattdessen, die folgenden Befehle auszuführen und achten Sie darauf, *<domain>* durch den richtigen Domänennamen für Ihre WordPress Multisite zu ersetzen.
>
> ```
> cd /opt/bitnami/apps/wordpress
> sudo ./bnconfig --machine_hostname <domain>
> ```
>
> Nachdem dieser Befehl ausgeführt wurde, geben Sie den folgenden Befehl ein, um zu verhindern, dass das bnconfig-Tool bei jedem Neustart des Servers automatisch ausgeführt wird.
>
> ```
> sudo mv bnconfig bnconfig.disabled
> ```

Nun sollte Sie das Navigieren im Browser zur von Ihnen definierten Domäne zum Hauptblog Ihrer WordPress Multisite-Instance umleiten.

Nächste Schritte

Führen Sie die nächsten Schritte aus, nachdem Sie die primäre Domäne für Ihre WordPress Multisite-Instance definiert haben:

- Blogs als Subdomains zu Ihrer WordPress-Multisite-Instance hinzufügen
- Blogs als Domains zu Ihrer WordPress Multisite-Instance hinzufügen

Tutorials zu Let's Encrypt für Amazon Lightsail

Let's Encrypt stellt kostenlose SSL/TLS-Zertifikate aus und ermöglicht so eine sichere und verschlüsselte Kommunikation für Websites, Anwendungen und Onlineservices. In den folgenden Tutorials erfahren Sie, wie Sie mit Let's Encrypt in Lightsail arbeiten.

Themen

- Tutorial: Verwenden von Let's-Encrypt-SSL-Zertifikaten mit Ihrer LAMP-Instance in Lightsail
- Tutorial: Verwenden von Let's-Encrypt-SSL-Zertifikaten mit Ihrer Nginx-Instance in Lightsail
- Tutorial: Verwenden Sie Let's Encrypt SSL-Zertifikate mit Ihrer WordPress Lightsail-Instanz

Tutorial: Verwenden von Let's-Encrypt-SSL-Zertifikaten mit Ihrer LAMP-Instance in Lightsail

Amazon Lightsail macht es einfach, Ihre Websites und Anwendungen mit SSL/TLS mit Lightsail-Load Balancer zu sichern. Ein Lightsail-Load Balancer muss jedoch nicht in jedem Fall die richtige Wahl sein. Möglicherweise benötigt Ihre Website nicht die Skalierbarkeit oder Fehlertoleranz, die Load Balancer bieten, oder vielleicht möchten Sie die Kosten optimieren.

Im letzteren Fall können Sie Let's Encrypt verwenden, um ein kostenloses SSL-Zertifikat zu erhalten. Wenn dies der Fall ist, ist das kein Problem. Sie können diese Zertifikate mit Lightsail-Instances integrieren. In diesem Tutorial erfahren Sie, wie Sie ein Let's Encrypt Wildcard-Zertifikat mit Certbot anfordern und in Ihre LAMP-Instance integrieren können.

> **Important**
>
> - Die Linux-Verteilung, die von Bitnami-Instances verwendet wird, wurde im Juli 2020 von Ubuntu zu Debian geändert. Aufgrund dieser Änderung unterscheiden sich einige der

Schritte in diesem Tutorial abhängig von der Linux-Verteilung Ihrer Instance. Alle nach der Änderung erstellten Bitnami-Vorlagen-Instances verwenden die Debian-Linux-Verteilung. Instances, die vor der Änderung erstellt wurden, verwenden weiterhin die Ubuntu-Linux-Verteilung. Um die Verteilung Ihrer Instance zu überprüfen, führen Sie den `uname -a` -Befehl aus. Die Antwort zeigt entweder Ubuntu oder Debian als Linux-Verteilung Ihrer Instance an.

- Bitnami ist gerade dabei, die Dateistruktur für viele ihrer Stacks zu ändern. Die Dateipfade in diesem Tutorial können sich ändern, je nachdem, ob Ihr Bitnami-Stack native Linux-Systempakete (Ansatz A) verwendet oder ob es sich um eine eigenständige Installation handelt (Ansatz B). Führen Sie den folgenden Befehl aus, um Ihren Bitnami-Installationstyp zu identifizieren und den Ansatz, dem Sie folgen möchten, zu bestimmen:

  ```
  test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach
  A: Using system packages." || echo "Approach B: Self-contained
  installation."
  ```

Inhalt

Schritt 1: Erfüllen der Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies nicht ohnehin bereits der Fall ist:

- Erstellen Sie eine LAMP-Instance in Lightsail. Weitere Informationen finden Sie unter Erstellen einer Instance.

- Registrieren Sie einen Domänennamen und verschaffen Sie sich den administrativen Zugriff auf seine DNS-Datensätze. Weitere Informationen hierzu finden Sie unter Amazon Lightsail-DNS.

  > **Note**
  >
  > Wir empfehlen Ihnen, die DNS-Datensätze Ihrer Domäne über eine Lightsail-DNS-Zone zu verwalten. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.

- Benutzen Sie das browserbasierte SSH-Terminal in der Lightsail-Konsole, um die Schritte in diesem Tutorial durchzuführen. Sie können aber auch Ihren eigenen SSH-Client verwenden, wie z. B. PuTTY. Informationen dazu, wie Sie PuTTY konfigurieren, finden Sie unter PuTTY herunterladen und einrichten, um eine Verbindung über SSH herzustellen.

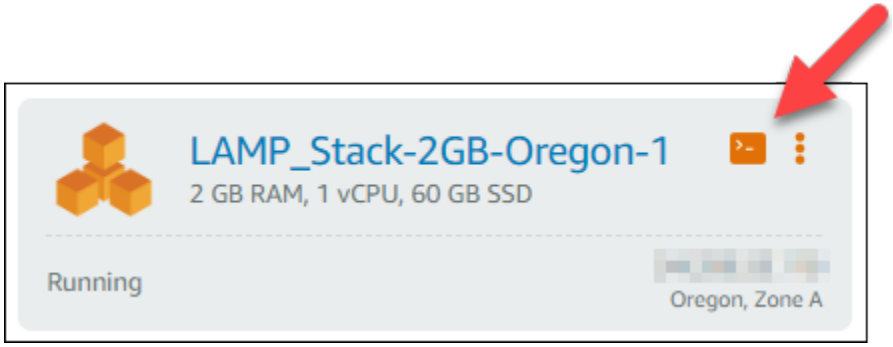
Nachdem Sie die Voraussetzungen erfüllt haben, fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 2: Installieren von Certbot auf Ihrer Instance

Certbot ist ein Client, mit dem ein Zertifikat von Let's Encrypt angefordert und auf einem Webserver bereitgestellt wird. Let's Encrypt verwendet das ACME-Protokoll, um Zertifikate auszustellen, und Certbot ist ein ACME-fähiger Client, der mit Let's Encrypt interagiert.

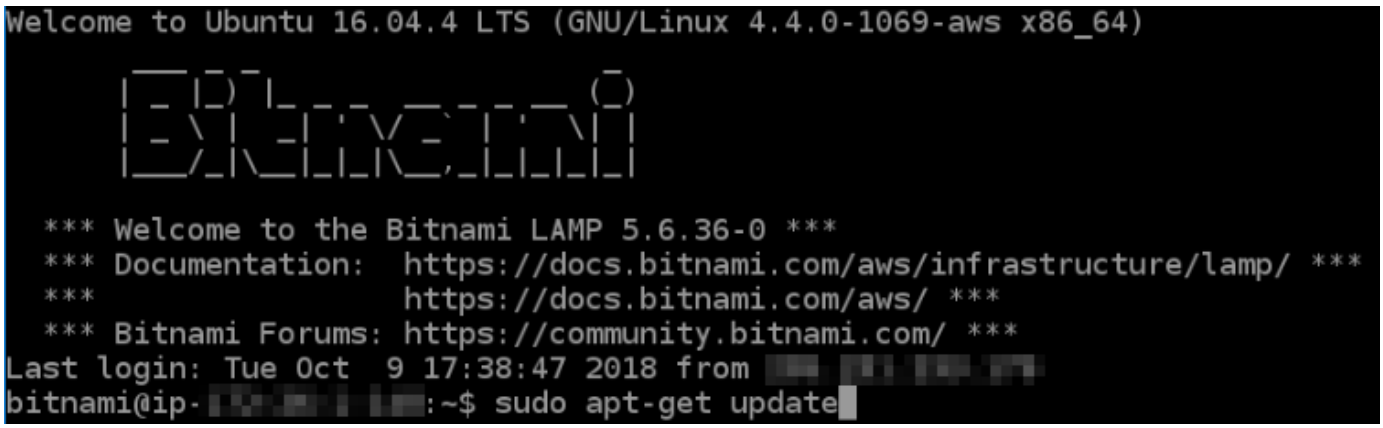
Um Certbot auf Ihrer Lightsail-Instance zu installieren

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Startseite von Lightsail das SSH-Schnellverbindungssymbol für die Instance, mit der Sie sich verbinden möchten.



3. Nachdem Ihre Lightsail browserbasierte SSH-Sitzung verbunden ist, geben Sie den folgenden Befehl ein, um die Pakete auf Ihrer Instance zu aktualisieren:

```
sudo apt-get update
```



4. Geben Sie den folgenden Befehl ein, um das Software-Eigenschaftenpaket zu installieren. Die Entwickler von Certbot verwenden ein Personal Package Archive (PPA), um Certbot zu verteilen. Das Software-Eigenschaftenpaket macht es effizienter, mit PPAs zu arbeiten.

```
sudo apt-get install software-properties-common
```

> **Note**
>
> Wenn ein `Could not get lock`-Fehler auftritt, wenn Sie den `sudo apt-get install`-Befehl ausführen, warten Sie etwa 15 Minuten und versuchen Sie es erneut. Dieser Fehler kann durch einen Cron-Job verursacht werden, der das Apt-Paketverwaltungstool verwendet, um unbeaufsichtigte Aktualisierungen zu installieren.

5. Geben Sie den folgenden Befehl ein, um Certbot zum lokalen apt-Repository hinzuzufügen:

> **Note**
>
> Schritt 5 gilt nur für Instances, die die Ubuntu-Linux-Verteilung verwenden. Überspringen Sie diesen Schritt, wenn Ihre Instance die Debian-Linux-Verteilung verwendet.

```
sudo apt-add-repository ppa:certbot/certbot -y
```

6. Geben Sie den folgenden Befehl ein, um apt zu aktualisieren und das neue Repository aufzunehmen:

```
sudo apt-get update -y
```

7. Geben Sie den folgenden Befehl ein, um Certbot zu installieren.

```
sudo apt-get install certbot -y
```

Certbot ist jetzt auf Ihrer Lightsail-Instance installiert.

8. Halten Sie das browserbasierte SSH-Terminalfenster geöffnet - Sie kehren später in diesem Tutorial dorthin zurück. Fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 3: Anfordern eines Let's Encrypt SSL Wildcard-Zertifikats

Beginnen Sie mit der Anforderung eines Zertifikats von Let's Encrypt. Fordern Sie mit Certbot ein Wildcard-Zertifikat an, mit dem Sie ein einzelnes Zertifikat für eine Domäne und ihre Unterdomänen verwenden können. Ein einzelnes Wildcard-Zertifikat funktioniert beispielsweise für die Top-Level-Domäne `example.com` und die Unterdomänen `blog.example.com` und `stuff.example.com`.

So fordern Sie ein Let's Encrypt SSL Wildcard-Zertifikat an

1. Geben Sie in dem browserbasierten SSH-Terminalfenster, das Sie auch in Schritt 2 dieses Tutorials verwendet haben, die folgenden Befehle ein, um eine Umgebungsvariable für Ihre Domain festzulegen. Sie können nun Befehle effizienter kopieren und einfügen, um das Zertifikat zu erhalten.

```
DOMAIN=Domain
```

```
WILDCARD=*.$DOMAIN
```

Ersetzen Sie im Befehl *`Domain (Domäne)`* durch Ihren registrierten Domänennamen.

Beispiel:

```
DOMAIN=example.com
```

```
WILDCARD=*.$DOMAIN
```

2. Geben Sie den folgenden Befehl ein, um zu bestätigen, dass die Variablen die richtigen Werte zurückgeben:

```
echo $DOMAIN && echo $WILDCARD
```

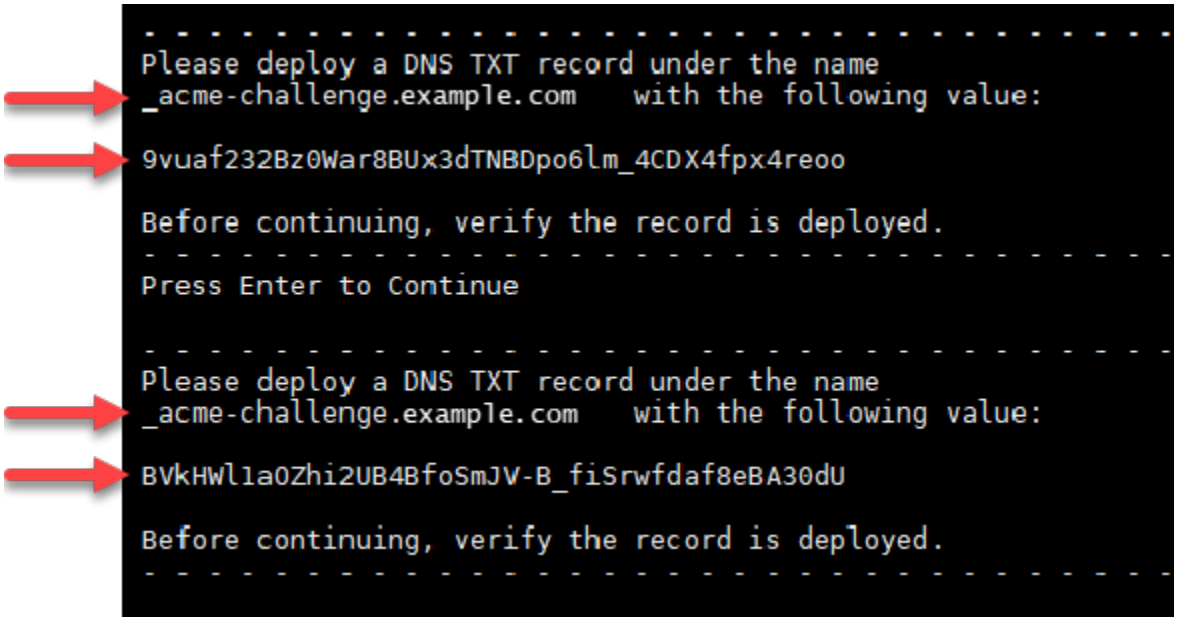
Das Ergebnis sollte in etwa wie folgt aussehen:

3. Geben Sie den folgenden Befehl ein, um Certbot im interaktiven Modus zu starten. Dieser Befehl weist Certbot an, eine manuelle Autorisierungsmethode mit DNS-Herausforderungen zu verwenden, um den Domänenbesitz zu überprüfen. Es fordert ein Wildcard-Zertifikat für Ihre Top-Level-Domäne sowie deren Unterdomänen an.

```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
```

4. Geben Sie bei Aufforderung Ihre E-Mail-Adresse ein, da sie für Verlängerungs- und Sicherheitshinweise verwendet wird.
5. Lesen Sie die Allgemeinen Geschäftsbedingungen von Let's Encrypt. Wenn Sie damit fertig sind, drücken Sie A, wenn Sie zustimmen. Wenn Sie nicht einverstanden sind, können Sie kein Let's Encrypt-Zertifikat erhalten.
6. Reagieren Sie entsprechend auf die Aufforderung, Ihre E-Mail-Adresse weiterzugeben, und auf die Warnung, dass Ihre IP-Adresse protokolliert wird.
7. Let's Encrypt fordert Sie jetzt auf, zu überprüfen, ob Sie die angegebene Domäne besitzen. Sie tun dies, indem Sie TXT-Einträge zu den DNS-Datensätzen für Ihre Domäne hinzufügen. Es wird ein Satz von TXT-Datensatzwerten bereitgestellt, wie im folgenden Beispiel gezeigt:

> **Note**
>
> Let's Encrypt kann einen einzelnen oder mehrere TXT-Datensätze bereitstellen, die Sie für die Verifizierung verwenden müssen. In diesem Beispiel wurden zwei TXT-Datensätze für die Verifizierung bereitgestellt.



8. Halten Sie die Lightsail browserbasierte SSH-Sitzung geöffnet - Sie kehren später in diesem Tutorial dorthin zurück. Fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 4: Hinzufügen von TXT-Datensätzen zur DNS-Zone Ihrer Domain

Wenn Sie einen TXT-Eintrag zur DNS-Zone Ihrer Domäne hinzufügen, wird überprüft, ob Sie die Domäne besitzen. Zu Demonstrationszwecken verwenden wir die DNS-Zone von Lightsail. Die Schritte können jedoch für andere DNS-Zonen ähnlich sein, die typischerweise von Domänen-Registraren gehostet werden.

> **Note**
>
> Weitere Informationen zum Erstellen einer Lightsail DNS-Zone für Ihre Domäne finden Sie unter Erstellen einer DNS-Zone für die Verwaltung Ihrer DNS-Datensätze in der Domäne in Lightsail.

So fügen Sie TXT-Einträge zur DNS-Zone Ihrer Domäne in Lightsail hinzu

1. Wählen Sie auf der Lightsail-Startseite die Registerkarte Domains & DNS (Domänen und DNS).
2. Wählen Sie im Abschnitt DNS zones (DNS-Zonen) auf der Seite die DNS-Zone für die Domäne aus, die Sie in der Certbot-Zertifikatsanforderung angegeben haben.

3. Wählen Sie im DNS-Zoneneditor die Registerkarte DNS records (DNS-Datensätze).
4. Wählen Sie Add record (Datensatz hinzufügen).
5. Wählen Sie im Dropdown-Menü Record type (Datensatztyp) die Option TXT record (TXT-Datensatz).
6. Geben Sie die in der Let's Encrypt-Zertifikatsanforderung angegebenen Werte in die Felder Record name (Datensatzname) und Responds with (Antwortet mit) ein.

> **Note**
>
> Die Lightsail-Konsole füllt den oberen Teil Ihrer Domäne vorab aus. Wenn Sie beispielsweise das *`_acme-challenge.example.com`*-Subdomain hinzufügen möchten, dann müssen Sie im Textfeld nur *`_acme-challenge`* eingeben und Lightsail fügt das `.example.com`-Teil für Sie hinzu, wenn Sie den Datensatz speichern.

7. Wählen Sie Save (Speichern).
8. Wiederholen Sie die Schritte 4 bis 7, um den zweiten Satz von TXT-Einträgen hinzuzufügen, der durch die Let's Encrypt-Zertifikatsanforderung spezifiziert wurde.
9. Halten Sie das Browserfenster der Lightsail-Konsole geöffnet - Sie kehren später in diesem Tutorial dorthin zurück. Fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 5: Bestätigen, dass die TXT-Datensätze weitergegeben wurden

Verwenden Sie das Dienstprogramm MxToolbox, um zu bestätigen, dass sich die TXT-Einträge über das DNS des Internets verbreitet haben. Die Verbreitung von DNS-Einträgen kann je nach Ihrem DNS-Hosting-Provider und der konfigurierten Lebenszeit (TTL - Time to Live) für Ihre DNS-Einträge eine Weile dauern. Es ist wichtig, dass Sie diesen Schritt abschließen und bestätigen, dass sich Ihre TXT-Einträge verbreitet haben, bevor Sie Ihre Certbot-Zertifikatsanforderung fortsetzen. Andernfalls schlägt Ihre Zertifikatsanforderung fehl.

So bestätigen Sie, dass sich die TXT-Einträge über das DNS des Internets verbreitet haben

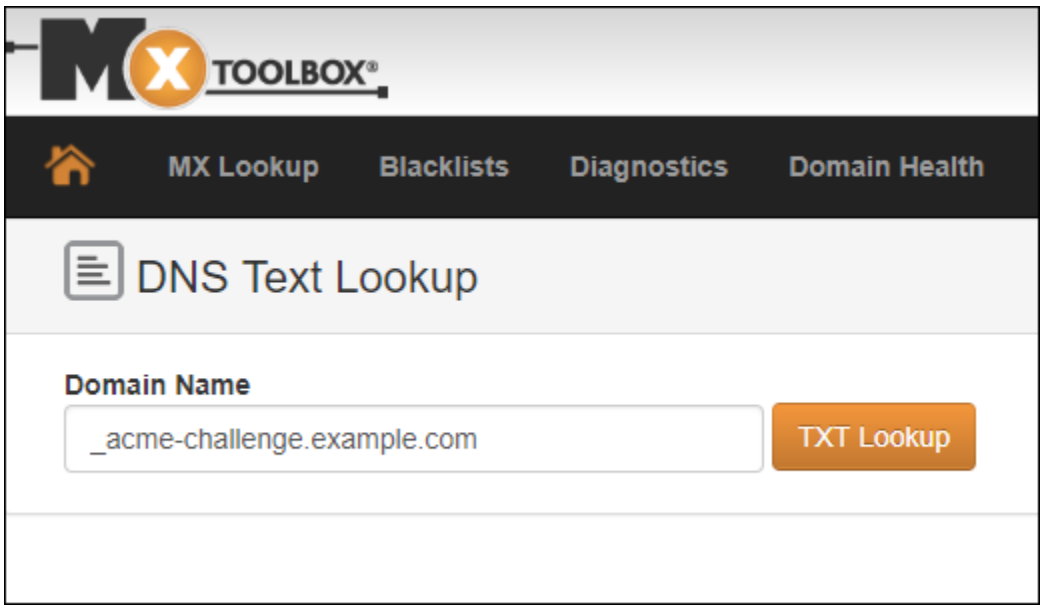
1. Öffnen Sie ein neues Browserfenster und gehen Sie zu https://mxtoolbox.com/TXTLookup.aspx.
2. Geben Sie den folgenden Text in das Textfeld ein.

```
_acme-challenge.Domain
```

Ersetzen Sie *Domain (Domäne)* durch Ihren registrierten Domainnamen.

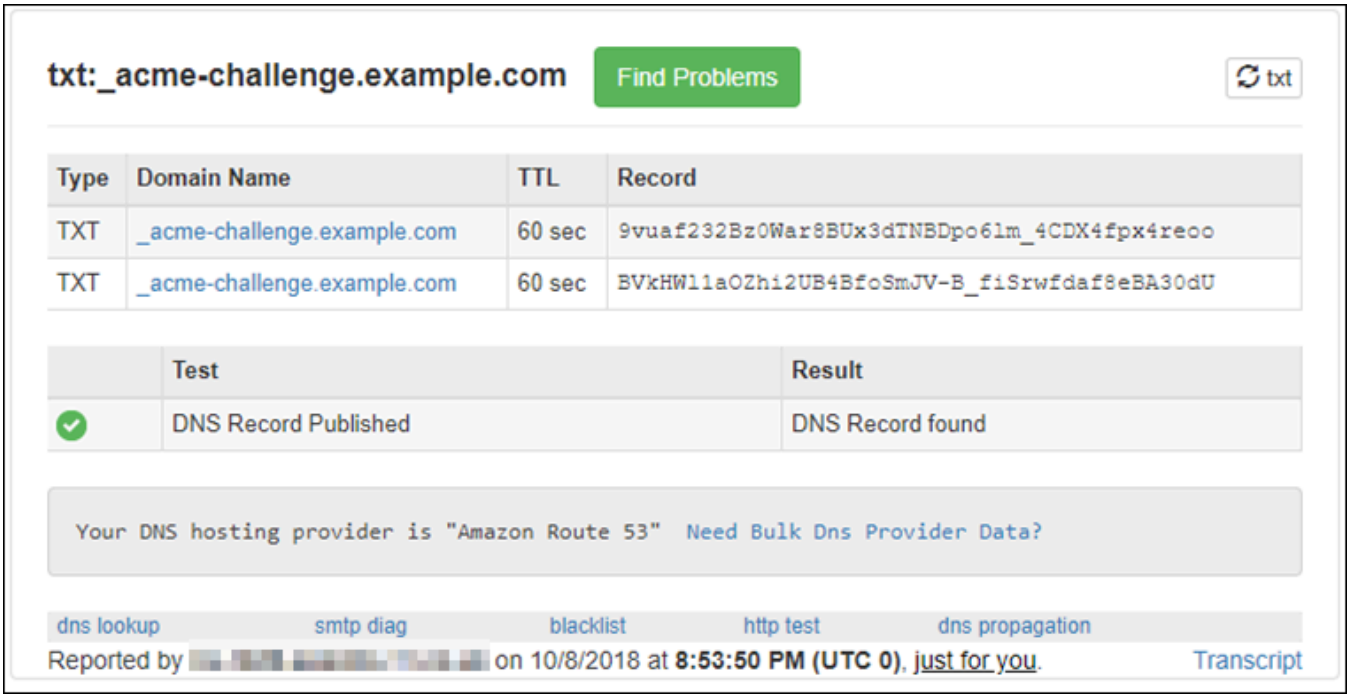
Beispiel:

```
_acme-challenge.example.com
```



3. Wählen Sie TXT Lookup (TXT-Suche), um die Prüfung auszuführen.
4. Eine der folgenden Antworten wird eintreten:

   - Wenn Ihre TXT-Datensätze an das DNS des Internets weitergegeben wurden, sehen Sie eine ähnliche Antwort wie im folgenden Screenshot. Schließen Sie das Browserfenster und fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.



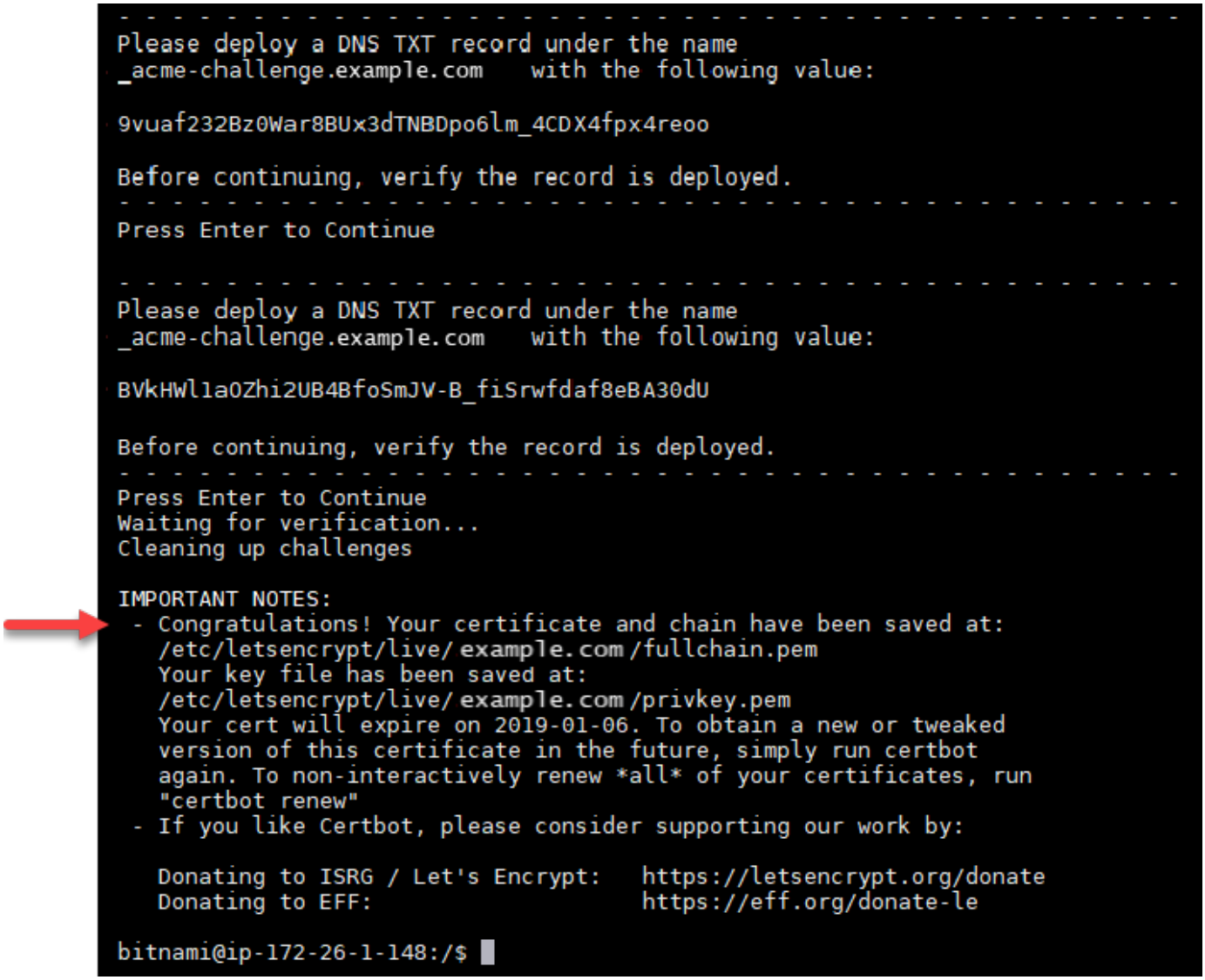
- Wenn Ihre TXT-Einträge nicht über das DNS des Internets verbreitet wurden, sehen Sie eine Antwort wie DNS Record not found (DNS-Datensatz nicht gefunden). Vergewissern Sie sich, dass Sie die richtigen DNS-Einträge zur DNS-Zone Ihrer Domäne hinzugefügt haben. Wenn Sie die richtigen Datensätze hinzugefügt haben, warten Sie noch eine Weile, bis sich die DNS-Einträge Ihrer Domäne verbreiten, und führen Sie die TXT-Suche erneut aus.

Schritt 6: Abschließen der Let's Encrypt SSL-Zertifikatsanforderung

Gehen Sie zurück zur Lightsail browserbasierten SSH-Sitzung für Ihre LAMP-Instance und schließen Sie die Let's Encrypt Zertifikatsanforderung ab. Certbot speichert Ihr SSL-Zertifikat, Ihre Kette und Ihre Schlüsseldateien in einem bestimmten Verzeichnis auf Ihrer LAMP-Instance.

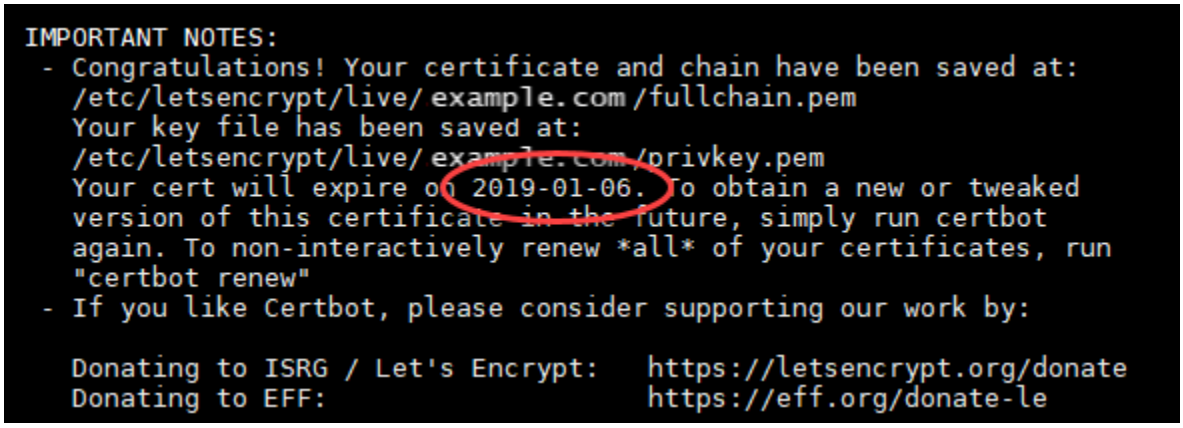
So schließen Sie die Let's Encrypt SSL-Zertifikatsanforderung ab

1. Drücken Sie in der Lightsail browserbasierten SSH-Sitzung für Ihre LAMP-Instance Enter (Eingabetaste), um Ihre Let's Encrypt SSL-Zertifikatsanforderung fortzusetzen. Bei Erfolg erscheint eine Antwort ähnlich der im folgenden Screenshot:



Die Nachricht bestätigt, dass Ihre Zertifikats-, Ketten- und Schlüsseldateien im Verzeichnis `/etc/letsencrypt/live/`*`Domain`*`/` gespeichert sind. *`Domain (Domäne)`* wird Ihr registrierter Domain-Name sein, z. B. `/etc/letsencrypt/live/`*`example.com`*`/`.

2. Notieren Sie sich das in der Nachricht angegebene Ablaufdatum. Sie verwenden es, um Ihr Zertifikat bis zu diesem Datum zu verlängern.



3. Da Sie nun das Let's Encrypt SSL-Zertifikat haben, fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 7: Erstellen von Links zu den Let's Encrypt-Zertifikatsdateien im Apache-Serververzeichnis

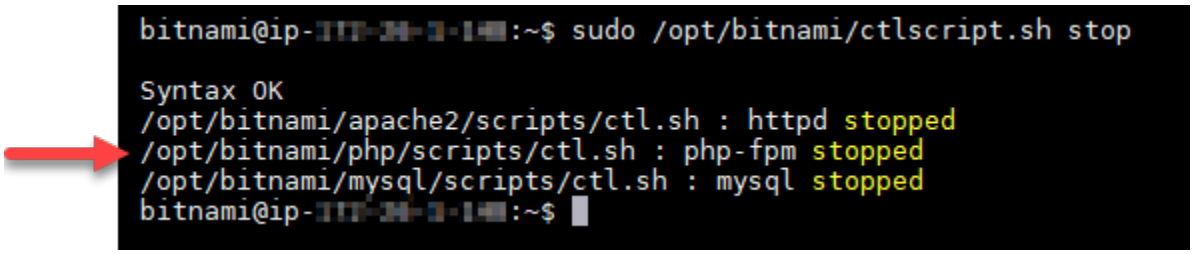
Erstellen Sie Links zu den SSL-Zertifikatsdateien von Let's Encrypt im Verzeichnis des Apache-Servers auf Ihrer LAMP-Instance. Außerdem sichern Sie Ihre vorhandenen Zertifikate, falls Sie sie später benötigen.

So erstellen Sie Links zu den Let's Encrypt-Zertifikatsdateien im Apache-Server-Verzeichnis

1. Geben Sie in der Lightsail browserbasierten SSH-Sitzung für Ihre LAMP-Instance den folgenden Befehl ein, um die zugrunde liegenden LAMP-Stapeldienste zu stoppen:

```
sudo /opt/bitnami/ctlscript.sh stop
```

Es wird eine Antwort ähnlich der folgenden angezeigt:



2. Geben Sie den folgenden Befehl ein, um eine Umgebungsvariable für Ihre Domäne zu setzen.

```
DOMAIN=Domain
```

Ersetzen Sie im Befehl *Domain (Domäne)* durch Ihren registrierten Domänennamen.

Beispiel:

```
DOMAIN=example.com
```

3. Geben Sie den folgenden Befehl ein, um zu bestätigen, dass die Variablen die richtigen Werte zurückgeben:

```
echo $DOMAIN
```

Das Ergebnis sollte in etwa wie folgt aussehen:

4. Geben Sie die folgenden Befehle einzeln ein, um Ihre vorhandenen Zertifikatsdateien als Backups umzubenennen. Informationen zu den verschiedenen Verteilungen und Dateistrukturen finden Sie im Abschnitt Wichtig am Anfang dieses Tutorials.

   - Für Debian-Linux-Verteilungen

     Ansatz A (Bitnami-Installationen mit Systempaketen):

     ```
     sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.crt /opt/bitnami/apache2/
     conf/bitnami/certs/server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.key /opt/bitnami/apache2/
     conf/bitnami/certs/server.key.old
     ```

     Ansatz B (Eigenständige Bitnami-Installationen):

     ```
     sudo mv /opt/bitnami/apache2/conf/server.crt /opt/bitnami/apache2/conf/
     server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/apache2/conf/server.key /opt/bitnami/apache2/conf/
     server.key.old
     ```

- Für ältere Instances, die die Ubuntu-Linux-Verteilung verwenden:

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.crt /opt/bitnami/apache/
conf/bitnami/certs/server.crt.old
```

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.key /opt/bitnami/apache/
conf/bitnami/certs/server.key.old
```

5. Geben Sie die folgenden Befehle einzeln ein, um Links zu Ihren Zertifikatsdateien von Let's Encrypt im Apache2–Server-Verzeichnis zu erstellen. Informationen zu den verschiedenen Verteilungen und Dateistrukturen finden Sie im Abschnitt Wichtig am Anfang dieses Tutorials.

   - Für Debian-Linux-Verteilungen

     Ansatz A (Bitnami-Installationen mit Systempaketen):

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/
bitnami/certs/server.key
```

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/
conf/bitnami/certs/server.crt
```

     Ansatz B (Eigenständige Bitnami-Installationen):

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/
server.key
```

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/
conf/server.crt
```

   - Für ältere Instances, die die Ubuntu-Linux-Verteilung verwenden:

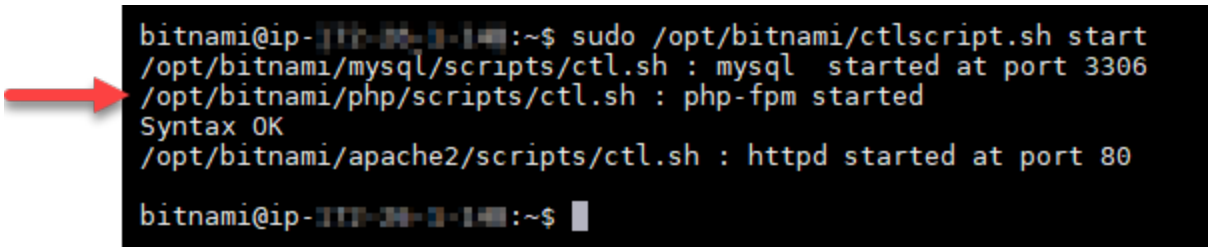
```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache/conf/
bitnami/certs/server.key
```

```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache/conf/
bitnami/certs/server.crt
```

6. Geben Sie den folgenden Befehl ein, um die zugrunde liegenden LAMP-Stapeldienste zu starten, die Sie zuvor gestoppt haben:

```
sudo /opt/bitnami/ctlscript.sh start
```

Das Ergebnis sollte in etwa wie folgt aussehen:



Ihre LAMP-Instance ist nun für die Verwendung der SSL-Verschlüsselung konfiguriert. Der Datenverkehr wird jedoch nicht automatisch von HTTP auf HTTPS umgeleitet.

7. Fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 8: Konfigurieren der HTTP zu HTTPS-Weiterleitung für Ihre Webanwendung

Sie können für Ihre LAMP-Instance eine HTTP-zu-HTTPS-Weiterleitung konfigurieren. Die automatische Umleitung von HTTP auf HTTPS macht Ihre Website nur Ihren Kunden über SSL zugänglich, auch wenn sie sich über HTTP verbinden.

So konfigurieren Sie die HTTP zu HTTPS Weiterleitung für Ihre Webanwendung

1. Geben Sie in der Lightsail browserbasierten SSH-Sitzung für Ihre LAMP-Instance den folgenden Befehl ein, um die Konfigurationsdatei des Apache Webservers mit dem Vim-Texteditor zu bearbeiten:

```
sudo vim /opt/bitnami/apache2/conf/bitnami/bitnami.conf
```

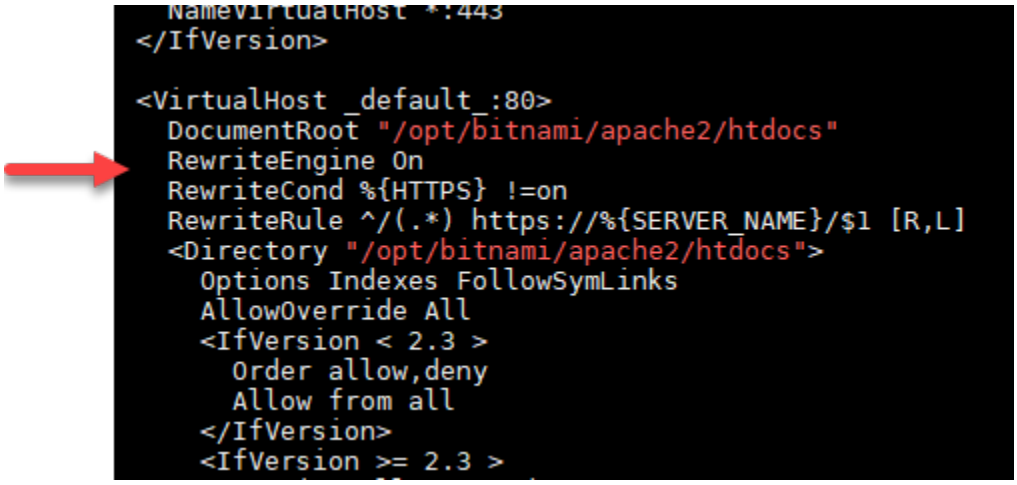
> **Note**
>
> Dieses Tutorial verwendet Vim zu Demonstrationszwecken, Sie können für diesen Schritt jedoch einen beliebigen Texteditor Ihrer Wahl verwenden.

2. Drücken Sie `i`, um in den Einfügemodus im Vim-Editor zu gelangen.

3. Geben Sie in der Datei den folgenden Text zwischen `DocumentRoot "/opt/bitnami/apache2/htdocs"` und `<Directory "/opt/bitnami/apache2/htdocs">` ein:

```
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^/(.*) https://%{SERVER_NAME}/$1 [R,L]
```

   Das Ergebnis sollte wie folgt aussehen:



4. Drücken Sie die Taste ESC, und geben Sie dann `:wq` ein, um Ihre Änderungen zu schreiben (speichern) und Vim zu beenden.
5. Geben Sie den folgenden Befehl ein, um die zugrunde liegenden LAMP-Stapeldienste neu zu starten und Ihre Änderungen wirksam zu machen:

```
sudo /opt/bitnami/ctlscript.sh restart
```

   Ihre LAMP-Instance ist jetzt so konfiguriert, dass Verbindungen automatisch von HTTP zu HTTPS umgeleitet werden. Wenn ein Besucher zu `http://www.example.com` geht, wird er automatisch an die verschlüsselte `https://www.example.com` Adresse weitergeleitet.

Schritt 9: Erneuern der Let's Encrypt Zertifikate alle 90 Tage

Die Zertifikate von Let's Encrypt sind 90 Tage lang gültig. Die Zertifikate können 30 Tage bevor sie ablaufen erneuert werden. Um die Let's Encrypt-Zertifikate zu erneuern, führen Sie den ursprünglichen Befehl aus, mit dem sie abgerufen wurden. Wiederholen Sie die Schritte im Abschnitt Anfordern eines Let's Encrypt SSL-Wildcard-Zertifikats in diesem Tutorial.

Tutorial: Verwenden von Let's-Encrypt-SSL-Zertifikaten mit Ihrer Nginx-Instance in Lightsail

Amazon Lightsail macht es einfach, Ihre Websites und Anwendungen mit SSL/TLS mit Lightsail-Load Balancer zu sichern. Ein Lightsail-Load Balancer muss jedoch nicht in jedem Fall die richtige Wahl sein. Möglicherweise benötigt Ihre Website nicht die Skalierbarkeit oder Fehlertoleranz, die Load Balancer bieten, oder vielleicht möchten Sie die Kosten optimieren.

Im letzteren Fall können Sie Let's Encrypt verwenden, um ein kostenloses SSL-Zertifikat zu erhalten. Wenn dies der Fall ist, ist das kein Problem. Sie können diese Zertifikate mit Lightsail-Instances integrieren. In diesem Tutorial erfahren Sie, wie Sie ein Let's Encrypt Wildcard-Zertifikat mit Certbot anfordern und in Ihre Nginx-Instance integrieren können.

Important

- Die Linux-Verteilung, die von Bitnami-Instances verwendet wird, wurde im Juli 2020 von Ubuntu zu Debian geändert. Aufgrund dieser Änderung unterscheiden sich einige der Schritte in diesem Tutorial abhängig von der Linux-Verteilung Ihrer Instance. Alle nach der Änderung erstellten Bitnami-Vorlagen-Instances verwenden die Debian-Linux-Verteilung. Instances, die vor der Änderung erstellt wurden, verwenden weiterhin die Ubuntu-Linux-Verteilung. Um die Verteilung Ihrer Instance zu überprüfen, führen Sie den `uname -a` -Befehl aus. Die Antwort zeigt entweder Ubuntu oder Debian als Linux-Verteilung Ihrer Instance an.
- Bitnami ist gerade dabei, die Dateistruktur für viele ihrer Stacks zu ändern. Die Dateipfade in diesem Tutorial können sich ändern, je nachdem, ob Ihr Bitnami-Stack native Linux-Systempakete (Ansatz A) verwendet oder ob es sich um eine eigenständige Installation handelt (Ansatz B). Führen Sie den folgenden Befehl aus, um Ihren Bitnami-Installationstyp zu identifizieren und den Ansatz, dem Sie folgen möchten, zu bestimmen:

  ```
  test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach
  A: Using system packages." || echo "Approach B: Self-contained
  installation."
  ```

Inhalt

- Schritt 2: Installieren von Certbot auf Ihrer Lightsail-Instance
- Schritt 3: Anfordern eines Let's Encrypt SSL Wildcard-Zertifikats
- Schritt 4: Hinzufügen von TXT-Datensätzen zur DNS-Zone Ihrer Domain
- Schritt 5: Bestätigen, dass die TXT-Datensätze weitergegeben wurden
- Schritt 6: Abschließen der Let's Encrypt SSL-Zertifikatsanforderung
- Schritt 7: Erstellen von Links zu den Let's Encrypt-Zertifikatsdateien im Nginx-Serververzeichnis
- Schritt 8: Konfigurieren der HTTP zu HTTPS-Weiterleitung für Ihre Webanwendung
- Schritt 9: Erneuern der Let's Encrypt Zertifikate alle 90 Tage

Schritt 1: Erfüllen der Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies nicht ohnehin bereits der Fall ist:

- Erstellen Sie eine Nginx-Instance in Lightsail. Weitere Informationen finden Sie unter Erstellen einer Instance.
- Registrieren Sie einen Domänennamen und verschaffen Sie sich den administrativen Zugriff auf seine DNS-Datensätze. Weitere Informationen hierzu finden Sie unter DNS.

> **Note**
>
> Wir empfehlen Ihnen, die DNS-Datensätze Ihrer Domäne über eine Lightsail-DNS-Zone zu verwalten. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.

- Benutzen Sie das browserbasierte SSH-Terminal in der Lightsail-Konsole, um die Schritte in diesem Tutorial durchzuführen. Sie können aber auch Ihren eigenen SSH-Client verwenden, wie z. B. PuTTY. Informationen dazu, wie Sie PuTTY konfigurieren, finden Sie unter PuTTY herunterladen und einrichten, um eine Verbindung in Amazon Lightsail über SSH herzustellen.

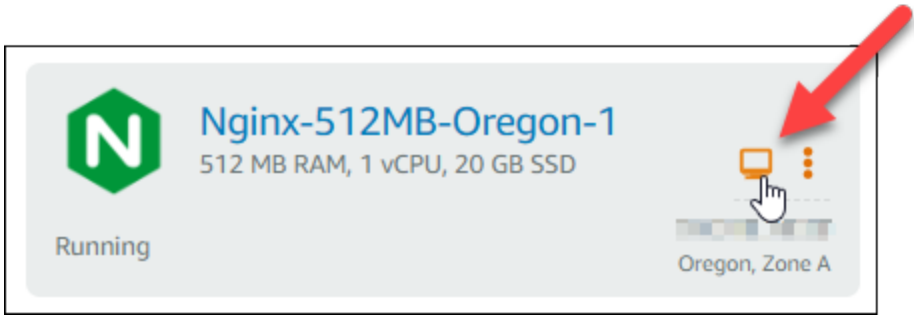
Nachdem Sie die Voraussetzungen erfüllt haben, fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 2: Installieren von Certbot auf Ihrer Lightsail-Instance

Certbot ist ein Client, mit dem ein Zertifikat von Let's Encrypt angefordert und auf einem Webserver bereitgestellt wird. Let's Encrypt verwendet das ACME-Protokoll, um Zertifikate auszustellen, und Certbot ist ein ACME-fähiger Client, der mit Let's Encrypt interagiert.

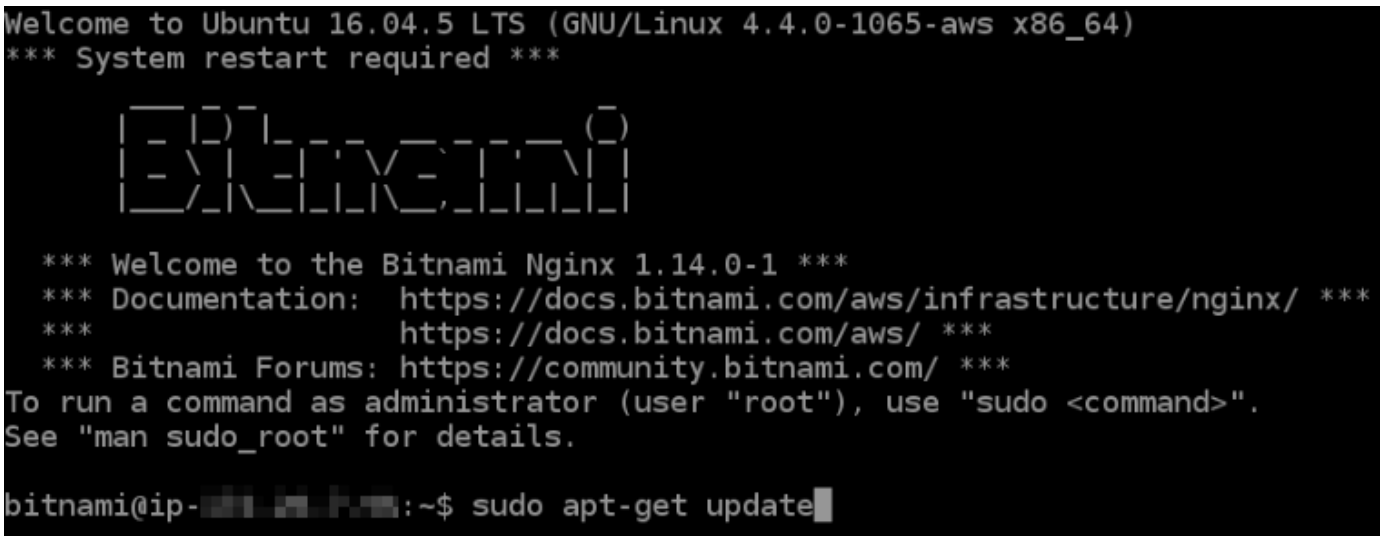
Um Certbot auf Ihrer Lightsail-Instance zu installieren

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Startseite von Lightsail das SSH-Schnellverbindungssymbol für die Instance, mit der Sie sich verbinden möchten.



3. Nachdem Ihre Lightsail browserbasierte SSH-Sitzung verbunden ist, geben Sie den folgenden Befehl ein, um die Pakete auf Ihrer Instance zu aktualisieren:

```
sudo apt-get update
```



4. Geben Sie den folgenden Befehl ein, um das Software-Eigenschaftenpaket zu installieren. Die Entwickler von Certbot verwenden ein Personal Package Archive (PPA), um Certbot zu verteilen. Das Software-Eigenschaftenpaket macht es effizienter, mit PPAs zu arbeiten.

```
sudo apt-get install software-properties-common
```

> **Note**
>
> Wenn ein `Could not get lock`-Fehler auftritt, wenn Sie den `sudo apt-get install`-Befehl ausführen, warten Sie etwa 15 Minuten und versuchen Sie es erneut. Dieser Fehler kann durch einen Cron-Job verursacht werden, der das Apt-Paketverwaltungstool verwendet, um unbeaufsichtigte Aktualisierungen zu installieren.

5. Geben Sie den folgenden Befehl ein, um Certbot zum lokalen apt-Repository hinzuzufügen:

> **Note**
>
> Schritt 5 gilt nur für Instances, die die Ubuntu-Linux-Verteilung verwenden. Überspringen Sie diesen Schritt, wenn Ihre Instance die Debian-Linux-Verteilung verwendet.

```
sudo apt-add-repository ppa:certbot/certbot -y
```

6. Geben Sie den folgenden Befehl ein, um apt zu aktualisieren und das neue Repository aufzunehmen:

```
sudo apt-get update -y
```

7. Geben Sie den folgenden Befehl ein, um Certbot zu installieren.

```
sudo apt-get install certbot -y
```

   Certbot ist jetzt auf Ihrer Lightsail-Instance installiert.

8. Halten Sie das browserbasierte SSH-Terminalfenster geöffnet - Sie kehren später in diesem Tutorial dorthin zurück. Fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 3: Anfordern eines Let's Encrypt SSL Wildcard-Zertifikats

Beginnen Sie mit der Anforderung eines Zertifikats von Let's Encrypt. Fordern Sie mit Certbot ein Wildcard-Zertifikat an, mit dem Sie ein einzelnes Zertifikat für eine Domäne und ihre Unterdomänen verwenden können. Ein einzelnes Wildcard-Zertifikat funktioniert beispielsweise für die Top-Level-Domäne `example.com` und die Unterdomänen `blog.example.com` und `stuff.example.com`.

So fordern Sie ein Let's Encrypt SSL Wildcard-Zertifikat an

1. Geben Sie in dem browserbasierten SSH-Terminalfenster, das Sie auch in Schritt 2 dieses Tutorials verwendet haben, die folgenden Befehle ein, um eine Umgebungsvariable für Ihre Domain festzulegen. Sie können nun Befehle effizienter kopieren und einfügen, um das Zertifikat zu erhalten. Achten Sie darauf, *`domain`* durch Ihren registrierten Domänennamen zu ersetzen.

   ```
   DOMAIN=domain
   ```

   ```
   WILDCARD=*.$DOMAIN
   ```

   Beispiel:

   ```
   DOMAIN=example.com
   ```

   ```
   WILDCARD=*.$DOMAIN
   ```

2. Geben Sie den folgenden Befehl ein, um zu bestätigen, dass die Variablen die richtigen Werte zurückgeben:

   ```
   echo $DOMAIN && echo $WILDCARD
   ```

   Das Ergebnis sollte in etwa wie folgt aussehen:

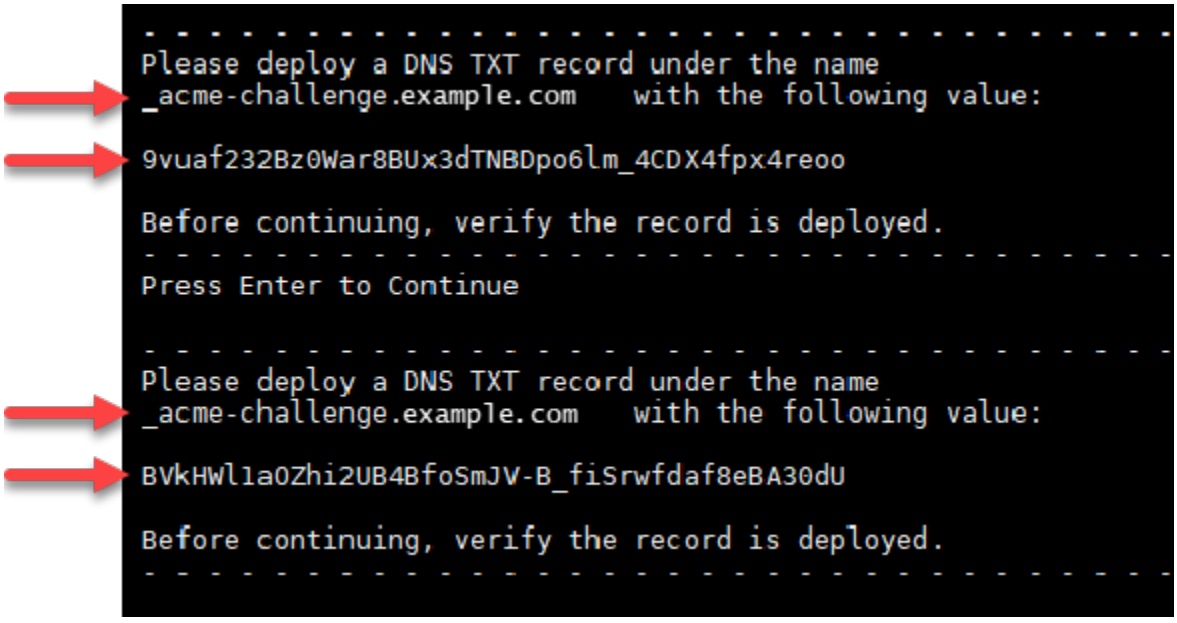
3. Geben Sie den folgenden Befehl ein, um Certbot im interaktiven Modus zu starten. Dieser Befehl weist Certbot an, eine manuelle Autorisierungsmethode mit DNS-Herausforderungen zu

verwenden, um den Domänenbesitz zu überprüfen. Es fordert ein Wildcard-Zertifikat für Ihre Top-Level-Domäne sowie deren Unterdomänen an.

```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
```

4. Geben Sie bei Aufforderung Ihre E-Mail-Adresse ein, da sie für Verlängerungs- und Sicherheitshinweise verwendet wird.
5. Lesen Sie die Allgemeinen Geschäftsbedingungen von Let's Encrypt. Wenn Sie damit fertig sind, drücken Sie A, wenn Sie zustimmen. Wenn Sie nicht einverstanden sind, können Sie kein Let's Encrypt-Zertifikat erhalten.
6. Reagieren Sie entsprechend auf die Aufforderung, Ihre E-Mail-Adresse weiterzugeben, und auf die Warnung, dass Ihre IP-Adresse protokolliert wird.
7. Let's Encrypt fordert Sie jetzt auf, zu überprüfen, ob Sie die angegebene Domäne besitzen. Sie tun dies, indem Sie TXT-Einträge zu den DNS-Datensätzen für Ihre Domäne hinzufügen. Es wird ein Satz von TXT-Datensatzwerten bereitgestellt, wie im folgenden Beispiel gezeigt:

> **Note**
>
> Let's Encrypt kann einen einzelnen oder mehrere TXT-Datensätze bereitstellen, die Sie für die Verifizierung verwenden müssen. In diesem Beispiel wurden zwei TXT-Datensätze für die Verifizierung bereitgestellt.



8. Halten Sie die Lightsail browserbasierte SSH-Sitzung geöffnet - Sie kehren später in diesem Tutorial dorthin zurück. Fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 4: Hinzufügen von TXT-Datensätzen zur DNS-Zone Ihrer Domain

Wenn Sie einen TXT-Eintrag zur DNS-Zone Ihrer Domäne hinzufügen, wird überprüft, ob Sie die Domäne besitzen. Zu Demonstrationszwecken verwenden wir die DNS-Zone von Lightsail. Die Schritte können jedoch für andere DNS-Zonen ähnlich sein, die typischerweise von Domänen-Registraren gehostet werden.

> **Note**
>
> Weitere Informationen zum Erstellen einer Lightsail DNS-Zone für Ihre Domäne finden Sie unter Erstellen einer DNS-Zone für die Verwaltung Ihrer DNS-Datensätze in der Domäne in Lightsail.

So fügen Sie TXT-Einträge zur DNS-Zone Ihrer Domäne in Lightsail hinzu

1. Wählen Sie auf der Lightsail-Startseite die Registerkarte Domains & DNS (Domänen und DNS).
2. Wählen Sie im Abschnitt DNS zones (DNS-Zonen) auf der Seite die DNS-Zone für die Domäne aus, die Sie in der Certbot-Zertifikatsanforderung angegeben haben.
3. Wählen Sie im DNS-Zoneneditor die Registerkarte DNS records (DNS-Datensätze).
4. Wählen Sie Add record (Datensatz hinzufügen).
5. Wählen Sie im Dropdown-Menü Record type (Datensatztyp) die Option TXT record (TXT-Datensatz).
6. Geben Sie die in der Let's Encrypt-Zertifikatsanforderung angegebenen Werte in die Felder Record name (Datensatzname) und Responds with (Antwortet mit) ein.

   > **Note**
   >
   > Die Lightsail-Konsole füllt den oberen Teil Ihrer Domäne vorab aus. Wenn Sie beispielsweise das *`_acme-challenge.example.com`*-Subdomain hinzufügen möchten, dann müssen Sie im Textfeld nur *`_acme-challenge`* eingeben und Lightsail fügt das `.example.com`-Teil für Sie hinzu, wenn Sie den Datensatz speichern.

7. Wählen Sie Save (Speichern).

8. Wiederholen Sie die Schritte 4 bis 7, um den zweiten Satz von TXT-Einträgen hinzuzufügen, der durch die Let's Encrypt-Zertifikatsanforderung spezifiziert wurde.
9. Halten Sie das Browserfenster der Lightsail-Konsole geöffnet - Sie kehren später in diesem Tutorial dorthin zurück. Fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 5: Bestätigen, dass die TXT-Datensätze weitergegeben wurden

Verwenden Sie das Dienstprogramm MxToolbox, um zu bestätigen, dass sich die TXT-Einträge über das DNS des Internets verbreitet haben. Die Verbreitung von DNS-Einträgen kann je nach Ihrem DNS-Hosting-Provider und der konfigurierten Lebenszeit (TTL - Time to Live) für Ihre DNS-Einträge eine Weile dauern. Es ist wichtig, dass Sie diesen Schritt abschließen und bestätigen, dass sich Ihre TXT-Einträge verbreitet haben, bevor Sie Ihre Certbot-Zertifikatsanforderung fortsetzen. Andernfalls schlägt Ihre Zertifikatsanforderung fehl.

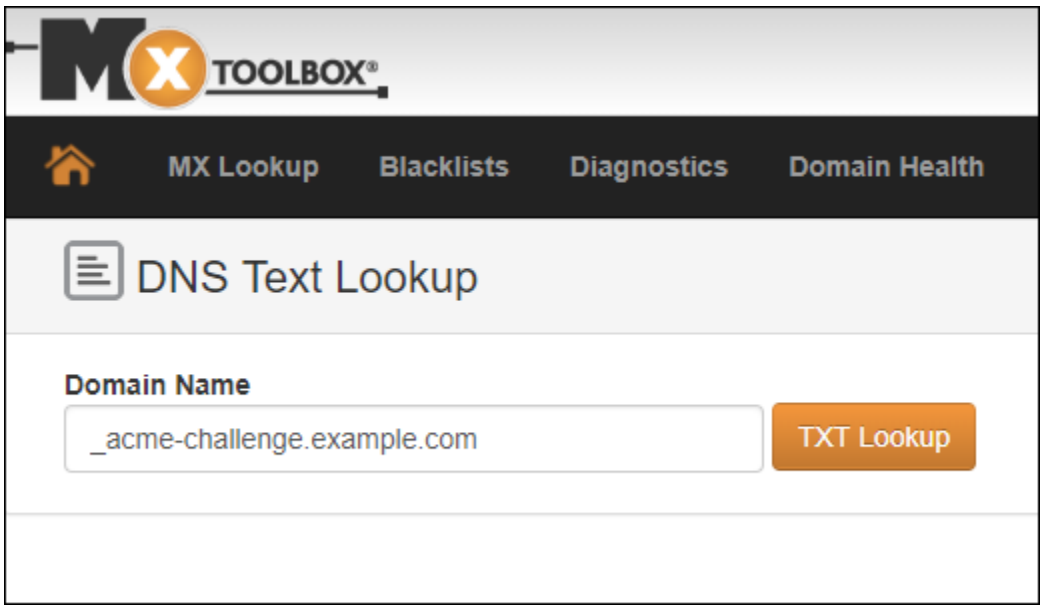
So bestätigen Sie, dass sich die TXT-Einträge über das DNS des Internets verbreitet haben

1. Öffnen Sie ein neues Browserfenster und gehen Sie zu https://mxtoolbox.com/TXTLookup.aspx.
2. Geben Sie den folgenden Text in das Textfeld ein. Stellen Sie sicher, dass Sie *domain* durch Ihre Domäne ersetzen.

   ```
   _acme-challenge.domain
   ```

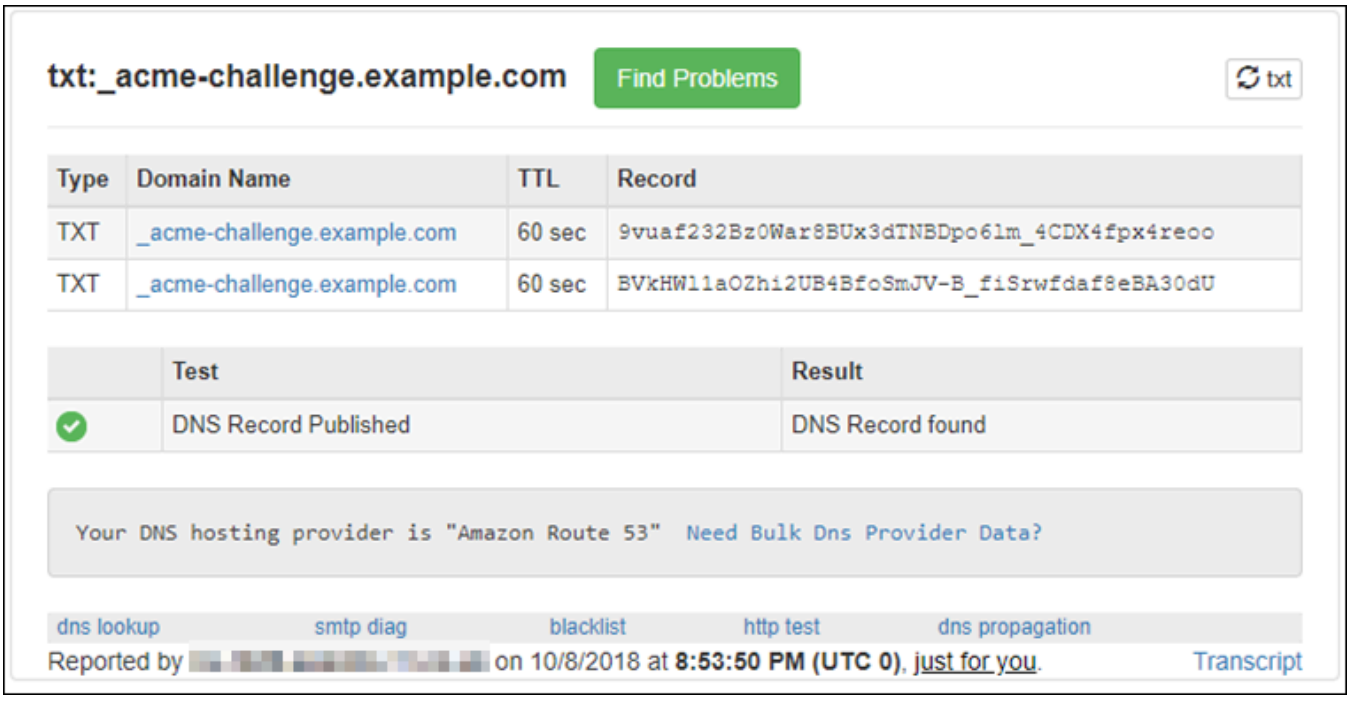
   Beispiel:

   ```
   _acme-challenge.example.com
   ```



3. Wählen Sie TXT Lookup (TXT-Suche), um die Prüfung auszuführen.
4. Eine der folgenden Antworten wird eintreten:

   - Wenn Ihre TXT-Datensätze an das DNS des Internets weitergegeben wurden, sehen Sie eine ähnliche Antwort wie im folgenden Screenshot. Schließen Sie das Browserfenster und fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.



   - Wenn Ihre TXT-Einträge nicht über das DNS des Internets verbreitet wurden, sehen Sie eine Antwort wie DNS Record not found (DNS-Datensatz nicht gefunden). Vergewissern Sie sich,

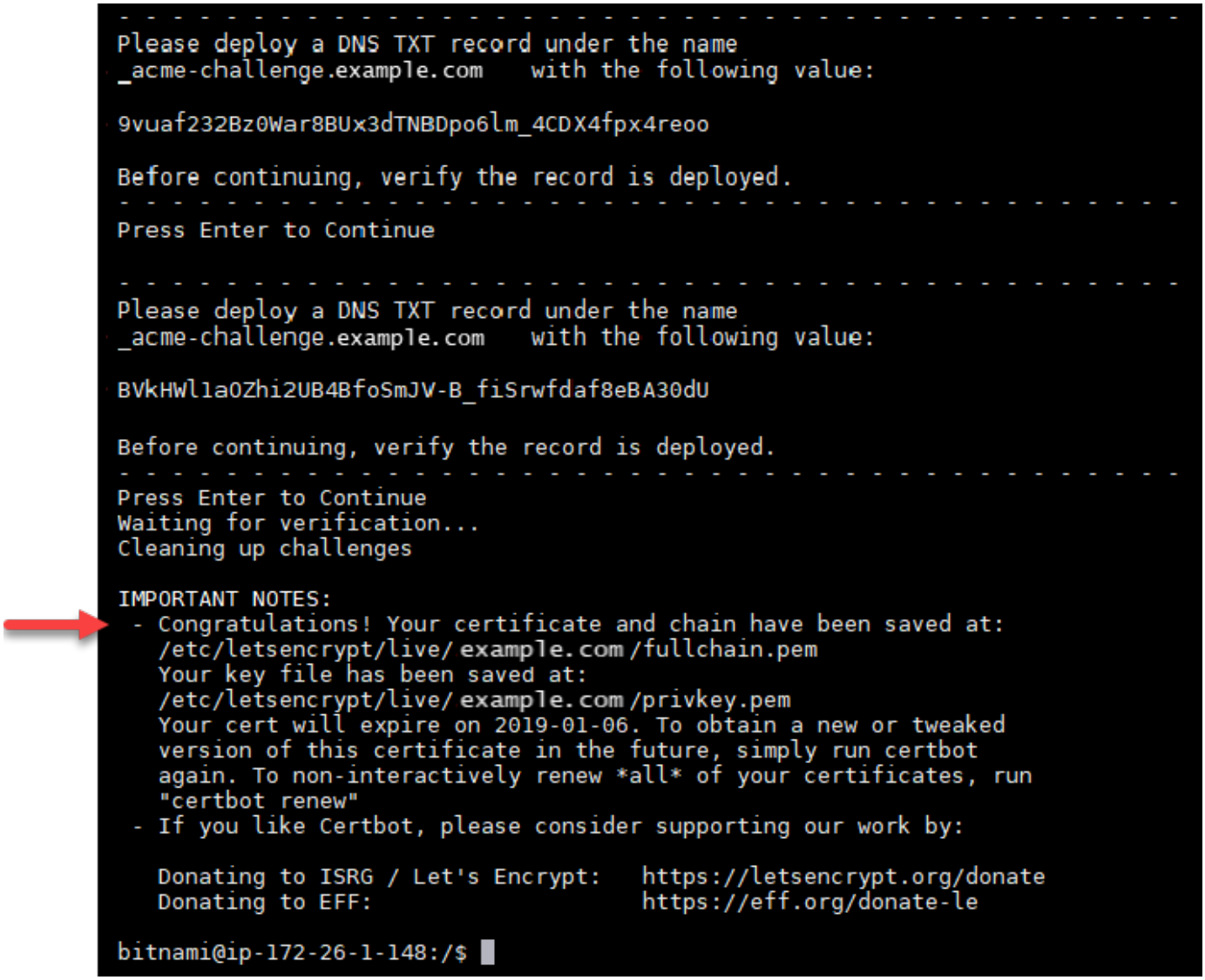
dass Sie die richtigen DNS-Einträge zur DNS-Zone Ihrer Domäne hinzugefügt haben. Wenn Sie die richtigen Datensätze hinzugefügt haben, warten Sie noch eine Weile, bis sich die DNS-Einträge Ihrer Domäne verbreiten, und führen Sie die TXT-Suche erneut aus.

Schritt 6: Abschließen der Let's Encrypt SSL-Zertifikatsanforderung

Gehen Sie zurück zur Lightsail browserbasierten SSH-Sitzung für Ihre Nginx-Instance und schließen Sie die Let's Encrypt Zertifikatsanforderung ab. Certbot speichert Ihr SSL-Zertifikat, Ihre Kette und Ihre Schlüsseldateien in einem bestimmten Verzeichnis auf Ihrer Nginx-Instance.

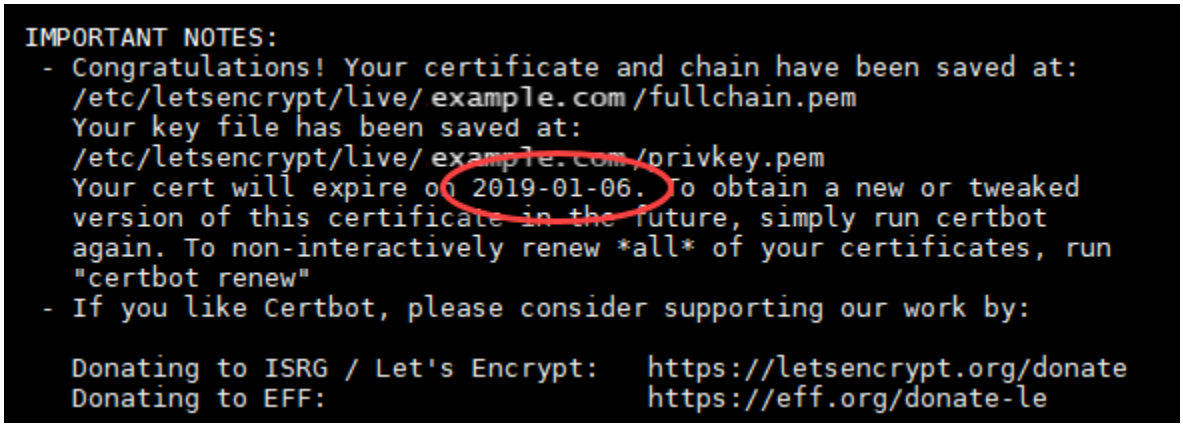
So schließen Sie die Let's Encrypt SSL-Zertifikatsanforderung ab

1. Drücken Sie in der Lightsail browserbasierten SSH-Sitzung für Ihre Nginx-Instance Enter (Eingabetaste), um Ihre Let's Encrypt SSL-Zertifikatsanforderung fortzusetzen. Bei Erfolg erscheint eine Antwort ähnlich der im folgenden Screenshot:



Die Nachricht bestätigt, dass Ihre Zertifikats-, Ketten- und Schlüsseldateien im Verzeichnis `/etc/letsencrypt/live/`*`domain`*`/` gespeichert sind. Stellen Sie sicher, dass Sie *`domain`* durch Ihre Domäne ersetzen, wie z. B. `/etc/letsencrypt/live/`*`example.com`*`/`.

2. Notieren Sie sich das in der Nachricht angegebene Ablaufdatum. Sie verwenden es, um Ihr Zertifikat bis zu diesem Datum zu verlängern.



3. Da Sie nun das Let's Encrypt SSL-Zertifikat haben, fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 7: Erstellen von Links zu den Let's Encrypt-Zertifikatsdateien im Nginx-Serververzeichnis

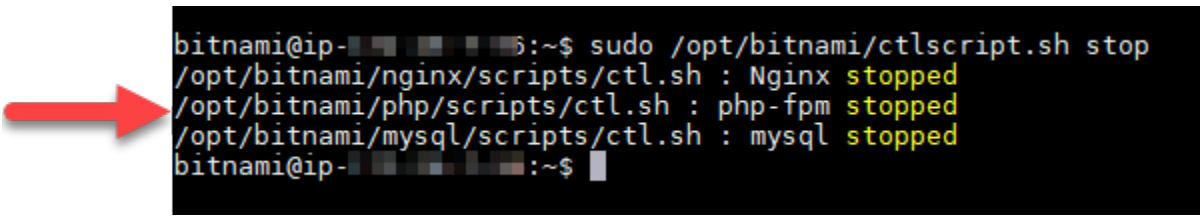
Erstellen Sie Links zu den Let's Encrypt SSL-Zertifikatsdateien im Nginx-Serververzeichnis auf Ihrer Nginx-Instance. Außerdem sichern Sie Ihre vorhandenen Zertifikate, falls Sie sie später benötigen.

So erstellen Sie Links zu den Let's Encrypt Zertifikatsdateien im Nginx-Serververzeichnis

1. Geben Sie in der Lightsail browserbasierten SSH-Sitzung für Ihre Nginx-Instance den folgenden Befehl ein, um die zugrunde liegenden LAMP-Stapeldienste zu stoppen:

```
sudo /opt/bitnami/ctlscript.sh stop
```

Es wird eine Antwort ähnlich der folgenden angezeigt:



2. Geben Sie den folgenden Befehl ein, um eine Umgebungsvariable für Ihre Domäne zu setzen. Sie können die Befehle effizienter kopieren und einfügen, um Ihre Zertifikatdateien zu verknüpfen. Achten Sie darauf, *domain* durch Ihre registrierte Domäne zu ersetzen.

```
DOMAIN=domain
```

Beispiel:

```
DOMAIN=example.com
```

3. Geben Sie den folgenden Befehl ein, um zu bestätigen, dass die Variablen die richtigen Werte zurückgeben:

```
echo $DOMAIN
```

Das Ergebnis sollte in etwa wie folgt aussehen:

4. Geben Sie die folgenden Befehle einzeln ein, um Ihre vorhandenen Zertifikatsdateien als Backups umzubenennen. Informationen zu den verschiedenen Verteilungen und Dateistrukturen finden Sie im Abschnitt Wichtig am Anfang dieses Tutorials.

   - Für Debian-Linux-Verteilungen

     Ansatz A (Bitnami-Installationen mit Systempaketen):

     ```
     sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.crt /opt/bitnami/nginx/conf/
     bitnami/certs/server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.key /opt/bitnami/nginx/conf/
     bitnami/certs/server.key.old
     ```

     Ansatz B (Eigenständige Bitnami-Installationen):

     ```
     sudo mv /opt/bitnami/nginx/conf/server.crt /opt/bitnami/nginx/conf/server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/nginx/conf/server.key /opt/bitnami/nginx/conf/server.key.old
     ```

   - Für ältere Instances, die die Ubuntu-Linux-Verteilung verwenden:

```
sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.crt /opt/bitnami/nginx/conf/
bitnami/certs/server.crt.old
```

```
sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.key /opt/bitnami/nginx/conf/
bitnami/certs/server.key.old
```

5. Geben Sie die folgenden Befehle einzeln ein, um Links zu Ihren Zertifikatsdateien von Let's Encrypt im Nginx-Verzeichnis zu erstellen. Informationen zu den verschiedenen Verteilungen und Dateistrukturen finden Sie im Abschnitt Wichtig am Anfang dieses Tutorials.

   - Für Debian-Linux-Verteilungen

     Ansatz A (Bitnami-Installationen mit Systempaketen):

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/nginx/conf/
     bitnami/certs/server.key
     ```

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/nginx/conf/
     bitnami/certs/server.crt
     ```

     Ansatz B (Eigenständige Bitnami-Installationen):

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/nginx/conf/
     server.key
     ```

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/nginx/conf/
     server.crt
     ```

   - Für ältere Instances, die die Ubuntu-Linux-Verteilung verwenden:

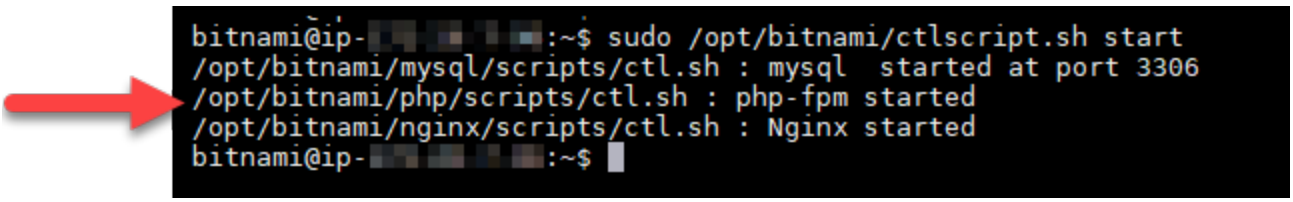
     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/nginx/conf/
     bitnami/certs/server.key
     ```

     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/nginx/conf/
     bitnami/certs/server.crt
     ```

6. Geben Sie den folgenden Befehl ein, um die zugrundeliegenden Services zu starten, die Sie zuvor gestoppt haben:

```
sudo /opt/bitnami/ctlscript.sh start
```

Das Ergebnis sollte in etwa wie folgt aussehen:



Ihre Nginx-Instance ist nun für die Verwendung der SSL-Verschlüsselung konfiguriert. Der Datenverkehr wird jedoch nicht automatisch von HTTP auf HTTPS umgeleitet.

7. Fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 8: Konfigurieren der HTTP zu HTTPS-Weiterleitung für Ihre Webanwendung

Sie können für Ihre Nginx-Instance eine HTTP-zu-HTTPS-Weiterleitung konfigurieren. Die automatische Umleitung von HTTP auf HTTPS macht Ihre Website nur Ihren Kunden über SSL zugänglich, auch wenn sie sich über HTTP verbinden. Informationen zu den verschiedenen Verteilungen und Dateistrukturen finden Sie im Abschnitt Wichtig am Anfang dieses Tutorials.

Dieses Tutorial verwendet Vim zu Demonstrationszwecken, Sie können jedoch einen beliebigen Texteditor Ihrer Wahl verwenden.

Für Debian-Linux-Verteilungen – Konfiguration der HTTP-zu-HTTPS-Weiterleitung für Ihre Webanwendung

1. Geben Sie in der browserbasierten Lightsail-SSH-Sitzung für Ihre Nginx-Instance den folgenden Befehl ein, um die Serverblock-Konfigurationsdatei zu ändern. Ersetzen Sie `<ApplicationName>` mit dem Namen Ihrer Anwendung.

   ```
   sudo vim /opt/bitnami/nginx/conf/server_blocks/<ApplicationName>-server-block.conf
   ```

2. Drücken Sie `i`, um in den Einfügemodus im Vim-Editor zu gelangen.
3. Bearbeiten Sie die Datei mit den Informationen aus dem folgenden Beispiel:

```
server {
    listen 80 default_server;
    root /opt/bitnami/APPNAME;
    return 301 https://$host$request_uri;
}
```

4. Drücken Sie die Taste ESC, und geben Sie dann `:wq` ein, um Ihre Änderungen zu schreiben (speichern) und Vim zu beenden.
5. Geben Sie den folgenden Befehl ein, um den Serverabschnitt der Nginx-Konfigurationsdatei zu ändern:

```
sudo vim /opt/bitnami/nginx/conf/nginx.conf
```

6. Drücken Sie `i`, um in den Einfügemodus im Vim-Editor zu gelangen.
7. Bearbeiten Sie die Datei mit den Informationen aus dem folgenden Beispiel:

```
server {
      listen 80;
      server_name localhost;
      return 301 https://$host$request_uri;
  }
```

8. Drücken Sie die Taste ESC, und geben Sie dann `:wq` ein, um Ihre Änderungen zu schreiben (speichern) und Vim zu beenden.
9. Geben Sie den folgenden Befehl ein, um die zugrunde liegenden Services neu zu starten und Ihre Änderungen wirksam zu machen:

```
sudo /opt/bitnami/ctlscript.sh restart
```

Ansatz B (Eigenständige Bitnami-Installationen):

1. Geben Sie in der Browser-basierten Lightsail-SSH-Sitzung für Ihre Nginx-Instance den folgenden Befehl ein, um den Server-Abschnitt der Nginx-Konfigurationsdatei zu ändern:

```
sudo vim /opt/bitnami/nginx/conf/nginx.conf
```

2. Drücken Sie `i`, um in den Einfügemodus im Vim-Editor zu gelangen.
3. Bearbeiten Sie die Datei mit den Informationen aus dem folgenden Beispiel:

```
server {
      listen 80;
      server_name localhost;
      return 301 https://$host$request_uri;
  }
```

4. Drücken Sie die Taste ESC, und geben Sie dann `:wq` ein, um Ihre Änderungen zu schreiben (speichern) und Vim zu beenden.
5. Geben Sie den folgenden Befehl ein, um die zugrunde liegenden Services neu zu starten und Ihre Änderungen wirksam zu machen:

```
sudo /opt/bitnami/ctlscript.sh restart
```

Für ältere Instances, die die Ubuntu-Linux-Verteilung verwenden – Konfigurieren der HTTP-zu-HTTPS-Weiterleitung für Ihre Webanwendung

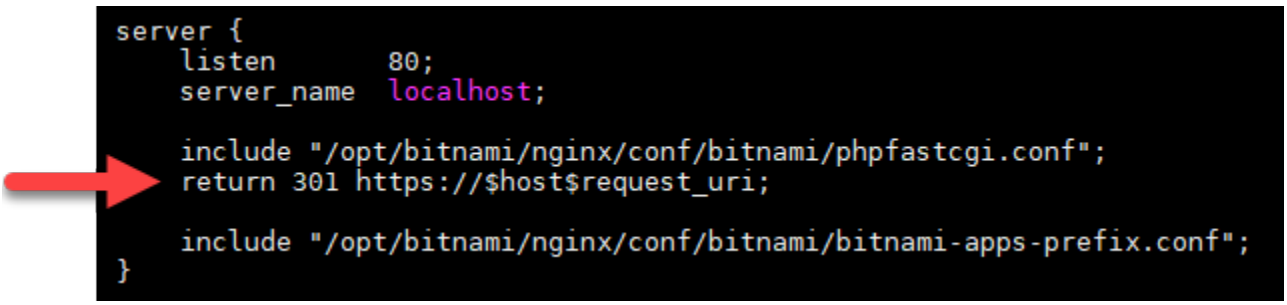
1. Geben Sie in der Lightsail browserbasierten SSH-Sitzung für Ihre Nginx-Instance den folgenden Befehl ein, um die Konfigurationsdatei des Nginx Webservers mit dem Vim-Texteditor zu bearbeiten:

```
sudo vim /opt/bitnami/nginx/conf/bitnami/bitnami.conf
```

2. Drücken Sie `i`, um in den Einfügemodus im Vim-Editor zu gelangen.
3. Geben Sie in der Datei den folgenden Text zwischen `server_name localhost;` und `include "/opt/bitnami/nginx/conf/bitnami/bitnami-apps-prefix.conf";` ein:

```
return 301 https://$host$request_uri;
```

   Das Ergebnis sollte wie folgt aussehen:



4. Drücken Sie die Taste ESC, und geben Sie dann `:wq` ein, um Ihre Änderungen zu schreiben (speichern) und Vim zu beenden.
5. Geben Sie den folgenden Befehl ein, um die zugrunde liegenden Services neu zu starten und Ihre Änderungen wirksam zu machen:

   ```
   sudo /opt/bitnami/ctlscript.sh restart
   ```

   Ihre Nginx-Instance ist jetzt so konfiguriert, dass Verbindungen automatisch von HTTP zu HTTPS umgeleitet werden. Wenn ein Besucher zu `http://www.example.com` geht, wird er automatisch an die verschlüsselte `https://www.example.com` Adresse weitergeleitet.

Schritt 9: Erneuern der Let's Encrypt Zertifikate alle 90 Tage

Die Zertifikate von Let's Encrypt sind 90 Tage lang gültig. Die Zertifikate können 30 Tage bevor sie ablaufen erneuert werden. Um die Let's Encrypt-Zertifikate zu erneuern, führen Sie den ursprünglichen Befehl aus, mit dem sie abgerufen wurden. Wiederholen Sie die Schritte im Abschnitt Anfordern eines Let's Encrypt SSL-Wildcard-Zertifikats in diesem Tutorial.

Tutorial: Verwenden Sie Let's Encrypt SSL-Zertifikate mit Ihrer WordPress Lightsail-Instanz

> **Tip**
>
> Lightsail bietet einen geführten Workflow, der die Installation und Konfiguration eines Let's Encrypt-Zertifikats auf Ihrer Instanz automatisiert. WordPress Wir empfehlen Ihnen dringend, den Workflow zu verwenden, anstatt die manuellen Schritte in diesem Tutorial zu befolgen. Weitere Informationen finden Sie unter Starten und Konfigurieren einer WordPress Instanz.

Amazon Lightsail macht es einfach, Ihre Websites und Anwendungen mithilfe von Lightsail-Load Balancern mit SSL/TLS zu sichern. Die Verwendung eines Lightsail-Loadbalancers ist jedoch im Allgemeinen möglicherweise nicht die richtige Wahl. Möglicherweise benötigt Ihre Website nicht die Skalierbarkeit oder Fehlertoleranz, die Load Balancer bieten, oder vielleicht möchten Sie die Kosten optimieren. Im letzteren Fall können Sie Let's Encrypt verwenden, um ein kostenloses SSL-Zertifikat zu erhalten. Wenn dies der Fall ist, ist das kein Problem. Sie können diese Zertifikate in Lightsail-Instances integrieren.

In dieser Anleitung erfahren Sie, wie Sie mit Certbot ein Let's Encrypt-Wildcard-Zertifikat anfordern und es mithilfe des Really Simple SSL-Plug-ins in Ihre WordPress Instanz integrieren.

- Die Linux-Verteilung, die von Bitnami-Instances verwendet wird, wurde im Juli 2020 von Ubuntu zu Debian geändert. Aufgrund dieser Änderung unterscheiden sich einige der Schritte in diesem Tutorial abhängig von der Linux-Verteilung Ihrer Instance. Alle nach der Änderung erstellten Bitnami-Vorlagen-Instances verwenden die Debian-Linux-Verteilung. Instances, die vor der Änderung erstellt wurden, verwenden weiterhin die Ubuntu-Linux-Verteilung. Um die Verteilung Ihrer Instance zu überprüfen, führen Sie den `uname -a` -Befehl aus. Die Antwort zeigt entweder Ubuntu oder Debian als Linux-Verteilung Ihrer Instance an.
- Bitnami hat die Dateistruktur für viele ihrer Stacks geändert. Die Dateipfade in diesem Tutorial können sich ändern, je nachdem, ob Ihr Bitnami-Stack native Linux-Systempakete (Ansatz A) verwendet oder ob es sich um eine eigenständige Installation handelt (Ansatz B). Führen Sie den folgenden Befehl aus, um Ihren Bitnami-Installationstyp zu identifizieren und den Ansatz, dem Sie folgen möchten, zu bestimmen:

  ```
  test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using system packages." || echo "Approach B: Self-contained installation."
  ```

Inhalt

Bevor Sie loslegen

Beachten Sie Folgendes, bevor Sie mit diesem Tutorial beginnen:

Verwenden Sie das Bitnami-HTTPS-Konfigurations (**`bncert`**)-Tool stattdessen

Die in diesem Tutorial beschriebenen Schritte zeigen Ihnen, wie Sie mithilfe eines manuellen Prozesses ein SSL-/TLS-Zertifikat implementieren. Bitnami bietet jedoch einen stärker automatisierten Prozess, der das Bitnami-HTTPS-Konfigurationstool (`bncert`) verwendet, das normalerweise auf Instanzen in Lightsail vorinstalliert ist. WordPress Wir empfehlen dringend, dieses Tool zu verwenden, anstatt die manuellen Schritte in diesem Tutorial zu befolgen. Dieses Tutorial wurde geschrieben, bevor das `bncert`-Tool verfügbar wurde. Weitere Informationen zur Verwendung des `bncert` Tools finden Sie unter HTTPS auf Ihrer WordPress Instance in Amazon Lightsail aktivieren.

Identifizieren Sie die Linux-Distribution Ihrer Instance WordPress

Die Linux-Verteilung, die von Bitnami-Instances verwendet wird, wurde im Juli 2020 von Ubuntu zu Debian geändert. Alle nach der Änderung erstellten Bitnami-Vorlagen-Instances verwenden die Debian-Linux-Verteilung. Instances, die vor der Änderung erstellt wurden, verwenden weiterhin die Ubuntu-Linux-Verteilung. Aufgrund dieser Änderung unterscheiden sich einige der Schritte in diesem Tutorial abhängig von der Linux-Verteilung Ihrer Instance. Sie müssen die Linux-Verteilung Ihrer Instance identifizieren, damit Sie wissen, welche Schritte in diesem Tutorial verwendet werden sollen. Um die Linux-Verteilung Ihrer Instance zu identifizieren, führen Sie den `uname -a` -Befehl aus. Die Antwort zeigt entweder Ubuntu oder Debian als Linux-Verteilung Ihrer Instance an.

Identifizieren Sie den Tutorial-Ansatz, der für Ihre Instance gilt

Bitnami ist gerade dabei, die Dateistruktur für viele ihrer Stacks zu ändern. Die Dateipfade in diesem Tutorial können sich ändern, je nachdem, ob Ihr Bitnami-Stack native Linux-Systempakete (Ansatz A) verwendet oder ob es sich um eine eigenständige Installation handelt (Ansatz B). Führen Sie den folgenden Befehl aus, um Ihren Bitnami-Installationstyp zu identifizieren und den Ansatz, dem Sie folgen möchten, zu bestimmen:

```
test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using
system packages." || echo "Approach B: Self-contained installation."
```

Schritt 1: Erfüllen der Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies nicht ohnehin bereits der Fall ist:

- Erstellen Sie eine WordPress Instanz in Lightsail. Weitere Informationen finden Sie unter Erstellen einer Instance.
- Registrieren Sie einen Domänennamen und verschaffen Sie sich den administrativen Zugriff auf seine DNS-Datensätze. Weitere Informationen hierzu finden Sie unter DNS.

  Wir empfehlen Ihnen, die DNS-Einträge Ihrer Domain mithilfe einer Lightsail-DNS-Zone zu verwalten. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.
- Verwenden Sie das browserbasierte SSH-Terminal in der Lightsail-Konsole, um die Schritte in diesem Tutorial auszuführen. Sie können aber auch Ihren eigenen SSH-Client verwenden, wie z. B. PuTTY. Weitere Informationen zur Konfiguration von PuTTY finden Sie unter PuTTY herunterladen und einrichten, um eine Verbindung über SSH in Amazon Lightsail herzustellen.

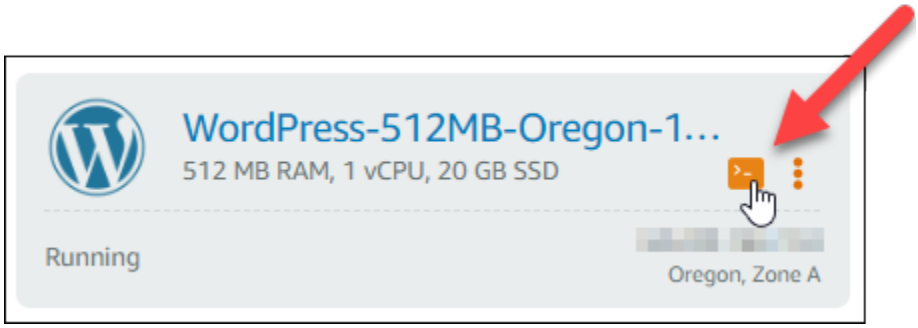
Nachdem Sie die Voraussetzungen erfüllt haben, fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 2: Installieren Sie Certbot auf Ihrer Lightsail-Instanz

Certbot ist ein Client, mit dem ein Zertifikat von Let's Encrypt angefordert und auf einem Webserver bereitgestellt wird. Let's Encrypt verwendet das ACME-Protokoll, um Zertifikate auszustellen, und Certbot ist ein ACME-fähiger Client, der mit Let's Encrypt interagiert.

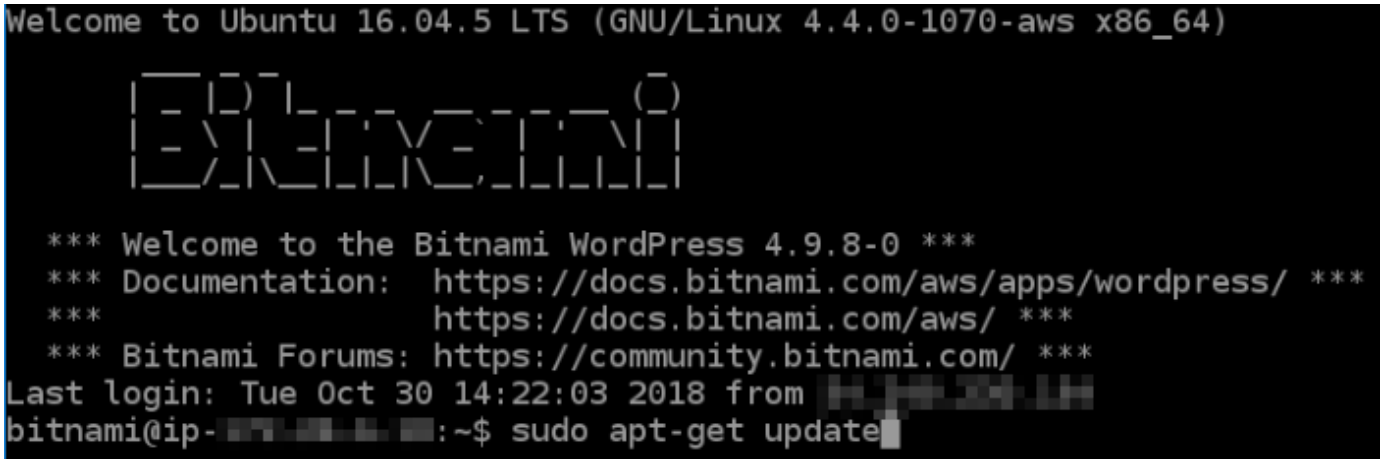
Um Certbot auf Ihrer Lightsail-Instanz zu installieren

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite das SSH-Schnellverbindungssymbol für die Instanz aus, zu der Sie eine Verbindung herstellen möchten.



3. Nachdem Ihre browserbasierte Lightsail-SSH-Sitzung verbunden ist, geben Sie den folgenden Befehl ein, um die Pakete auf Ihrer Instanz zu aktualisieren:

```
sudo apt-get update
```



4. Geben Sie den folgenden Befehl ein, um das Software-Eigenschaftenpaket zu installieren. Die Entwickler von Certbot verwenden ein Personal Package Archive (PPA), um Certbot zu verteilen. Das Software-Eigenschaftenpaket macht es effizienter, mit PPAs zu arbeiten.

```
sudo apt-get install software-properties-common
```

> **Note**
>
> Wenn ein `Could not get lock`-Fehler auftritt, wenn Sie den `sudo apt-get install`-Befehl ausführen, warten Sie etwa 15 Minuten und versuchen Sie es erneut. Dieser Fehler kann durch einen Cron-Job verursacht werden, der das Apt-Paketverwaltungstool verwendet, um unbeaufsichtigte Aktualisierungen zu installieren.

5. Geben Sie den folgenden Befehl ein, um Certbot zum lokalen apt-Repository hinzuzufügen:

> **Note**
>
> Schritt 5 gilt nur für Instances, die die Ubuntu-Linux-Verteilung verwenden. Überspringen Sie diesen Schritt, wenn Ihre Instance die Debian-Linux-Verteilung verwendet.

```
sudo apt-get install gpg -y
```

```
sudo apt-add-repository ppa:certbot/certbot -y
```

6. Geben Sie den folgenden Befehl ein, um apt zu aktualisieren und das neue Repository aufzunehmen:

```
sudo apt-get update -y
```

7. Geben Sie den folgenden Befehl ein, um Certbot zu installieren.

```
sudo apt-get install certbot -y
```

Certbot ist jetzt auf Ihrer Lightsail-Instanz installiert.

8. Halten Sie das browserbasierte SSH-Terminalfenster geöffnet - Sie kehren später in diesem Tutorial dorthin zurück. Fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 3: Anfordern eines Let's Encrypt SSL Wildcard-Zertifikats

Beginnen Sie mit der Anforderung eines Zertifikats von Let's Encrypt. Fordern Sie mit Certbot ein Wildcard-Zertifikat an, mit dem Sie ein einzelnes Zertifikat für eine Domäne und ihre Unterdomänen verwenden können. Ein einzelnes Wildcard-Zertifikat funktioniert beispielsweise für die Top-Level-Domäne `example.com` und die Unterdomänen `blog.example.com` und `stuff.example.com`.

So fordern Sie ein Let's Encrypt SSL Wildcard-Zertifikat an

1. Geben Sie in dem browserbasierten SSH-Terminalfenster, das Sie auch in Schritt 2 dieses Tutorials verwendet haben, die folgenden Befehle ein, um eine Umgebungsvariable für Ihre Domain festzulegen. Sie können nun Befehle effizienter kopieren und einfügen, um das Zertifikat zu erhalten. Achten Sie darauf, *`domain`* durch Ihre registrierte Domäne zu ersetzen.

```
DOMAIN=domain
```

```
WILDCARD=*.$DOMAIN
```

Beispiel:

```
DOMAIN=example.com
```

```
WILDCARD=*.$DOMAIN
```

2. Geben Sie den folgenden Befehl ein, um zu bestätigen, dass die Variablen die richtigen Werte zurückgeben:

```
echo $DOMAIN && echo $WILDCARD
```

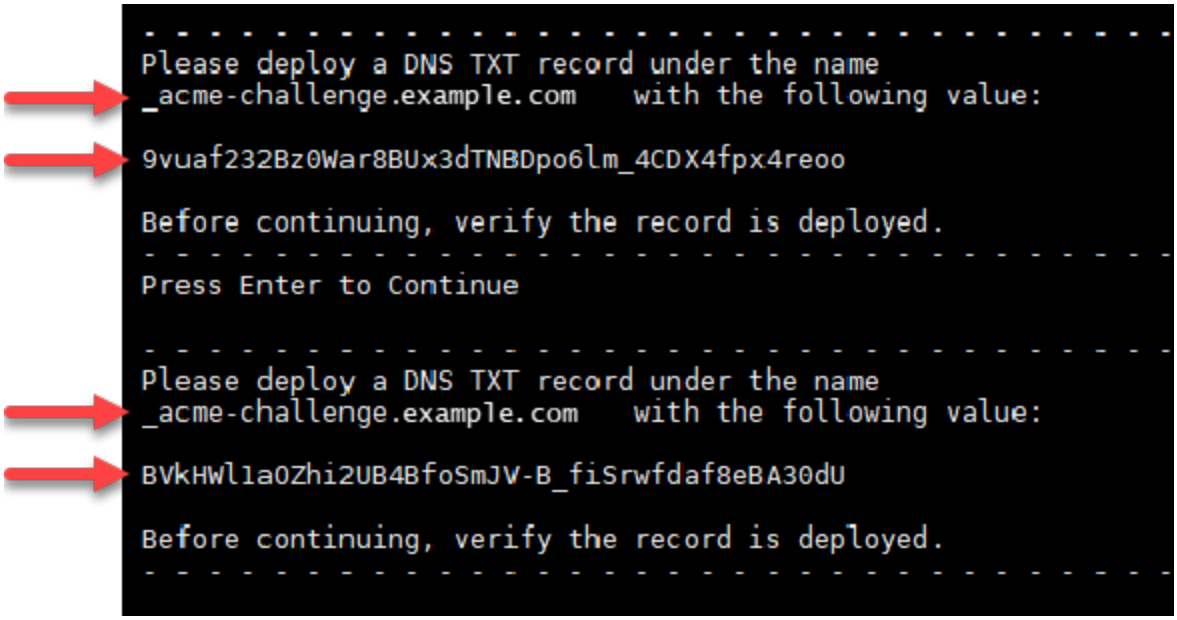
Das Ergebnis sollte in etwa wie folgt aussehen:

3. Geben Sie den folgenden Befehl ein, um Certbot im interaktiven Modus zu starten. Dieser Befehl weist Certbot an, eine manuelle Autorisierungsmethode mit DNS-Herausforderungen zu verwenden, um den Domänenbesitz zu überprüfen. Es fordert ein Wildcard-Zertifikat für Ihre Top-Level-Domäne sowie deren Unterdomänen an.

```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
```

4. Geben Sie bei Aufforderung Ihre E-Mail-Adresse ein, da sie für Verlängerungs- und Sicherheitshinweise verwendet wird.
5. Lesen Sie die Allgemeinen Geschäftsbedingungen von Let's Encrypt. Wenn Sie damit fertig sind, drücken Sie A, wenn Sie zustimmen. Wenn Sie nicht einverstanden sind, können Sie kein Let's Encrypt-Zertifikat erhalten.
6. Reagieren Sie entsprechend auf die Aufforderung, Ihre E-Mail-Adresse weiterzugeben, und auf die Warnung, dass Ihre IP-Adresse protokolliert wird.
7. Let's Encrypt fordert Sie jetzt auf, zu überprüfen, ob Sie die angegebene Domäne besitzen. Sie tun dies, indem Sie TXT-Einträge zu den DNS-Datensätzen für Ihre Domäne hinzufügen. Es wird ein Satz von TXT-Datensatzwerten bereitgestellt, wie im folgenden Beispiel gezeigt:

> **Note**
>
> Let's Encrypt kann einen einzelnen oder mehrere TXT-Datensätze bereitstellen, die Sie für die Verifizierung verwenden müssen. In diesem Beispiel wurden zwei TXT-Datensätze für die Verifizierung bereitgestellt.



8. Lassen Sie die browserbasierte Lightsail-SSH-Sitzung geöffnet — Sie werden später in diesem Tutorial darauf zurückkommen. Fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 4: Hinzufügen von TXT-Datensätzen zur DNS-Zone Ihrer Domain

Wenn Sie einen TXT-Eintrag zur DNS-Zone Ihrer Domäne hinzufügen, wird überprüft, ob Sie die Domäne besitzen. Zu Demonstrationszwecken verwenden wir die Lightsail-DNS-Zone. Die Schritte können jedoch für andere DNS-Zonen ähnlich sein, die typischerweise von Domänen-Registraren gehostet werden.

> **Note**
>
> Weitere Informationen zum Erstellen einer Lightsail-DNS-Zone für Ihre Domain finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Einträge Ihrer Domain in Lightsail.

Um TXT-Einträge zur DNS-Zone Ihrer Domain in Lightsail hinzuzufügen

1. Wählen Sie auf der Lightsail-Startseite die Registerkarte Domains & DNS (Domänen und DNS).
2. Wählen Sie im Abschnitt DNS zones (DNS-Zonen) auf der Seite die DNS-Zone für die Domäne aus, die Sie in der Certbot-Zertifikatsanforderung angegeben haben.
3. Wählen Sie im DNS-Zoneneditor die Registerkarte DNS records (DNS-Datensätze).
4. Wählen Sie Add record (Datensatz hinzufügen).
5. Wählen Sie im Dropdown-Menü Record type (Datensatztyp) die Option TXT record (TXT-Datensatz).
6. Geben Sie die in der Let's Encrypt-Zertifikatsanforderung angegebenen Werte in die Felder Record name (Datensatzname) und Responds with (Antwortet mit) ein.

   > **Note**
   >
   > Die Lightsail-Konsole füllt den oberen Teil Ihrer Domain vorab aus. Wenn Sie beispielsweise das *`_acme-challenge.example.com`*-Subdomain hinzufügen möchten, dann müssen Sie im Textfeld nur *`_acme-challenge`* eingeben und Lightsail fügt das `.example.com`-Teil für Sie hinzu, wenn Sie den Datensatz speichern.

7. Wählen Sie Speichern.
8. Wiederholen Sie die Schritte 4 bis 7, um den zweiten Satz von TXT-Einträgen hinzuzufügen, der durch die Let's Encrypt-Zertifikatsanforderung spezifiziert wurde.
9. Lassen Sie das Browserfenster der Lightsail-Konsole geöffnet — Sie werden später in diesem Tutorial darauf zurückkommen. Fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 5: Bestätigen, dass die TXT-Datensätze weitergegeben wurden

Verwenden Sie das MxToolbox Tool, um zu überprüfen, ob die TXT-Einträge an das DNS des Internets weitergegeben wurden. Die Verbreitung von DNS-Einträgen kann je nach Ihrem DNS-Hosting-Provider und der konfigurierten Lebenszeit (TTL - Time to Live) für Ihre DNS-Einträge eine Weile dauern. Es ist wichtig, dass Sie diesen Schritt abschließen und bestätigen, dass sich Ihre TXT-Einträge verbreitet haben, bevor Sie Ihre Certbot-Zertifikatsanforderung fortsetzen. Andernfalls schlägt Ihre Zertifikatsanforderung fehl.

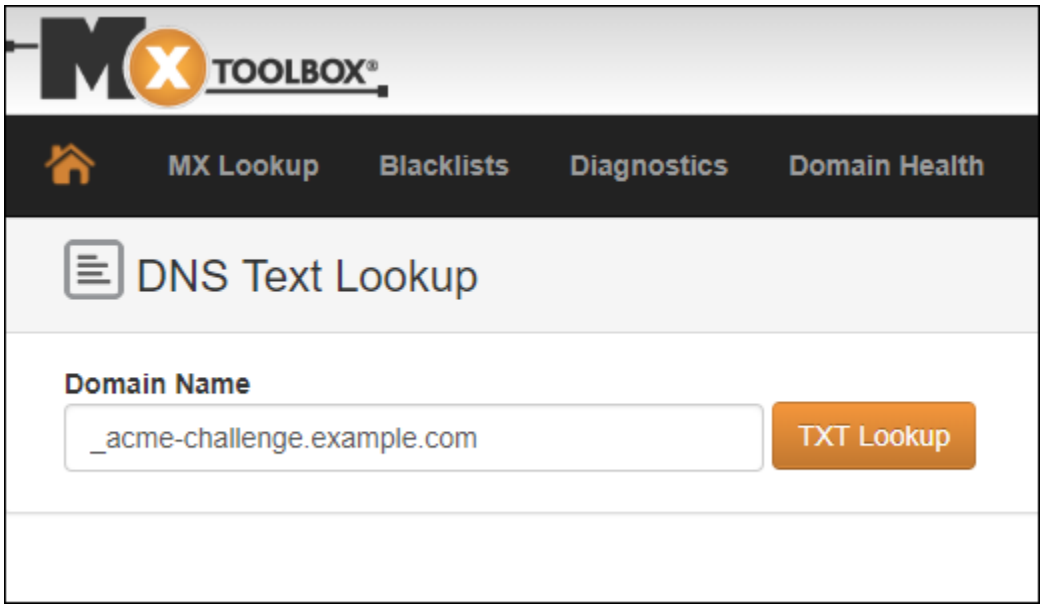
So bestätigen Sie, dass sich die TXT-Einträge über das DNS des Internets verbreitet haben

1. Öffnen Sie ein neues Browserfenster und gehen Sie zu https://mxtoolbox.com/TXTLookup.aspx.
2. Geben Sie den folgenden Text in das Textfeld ein. Stellen Sie sicher, dass Sie *domain* durch Ihre Domäne ersetzen.

   ```
   _acme-challenge.domain
   ```

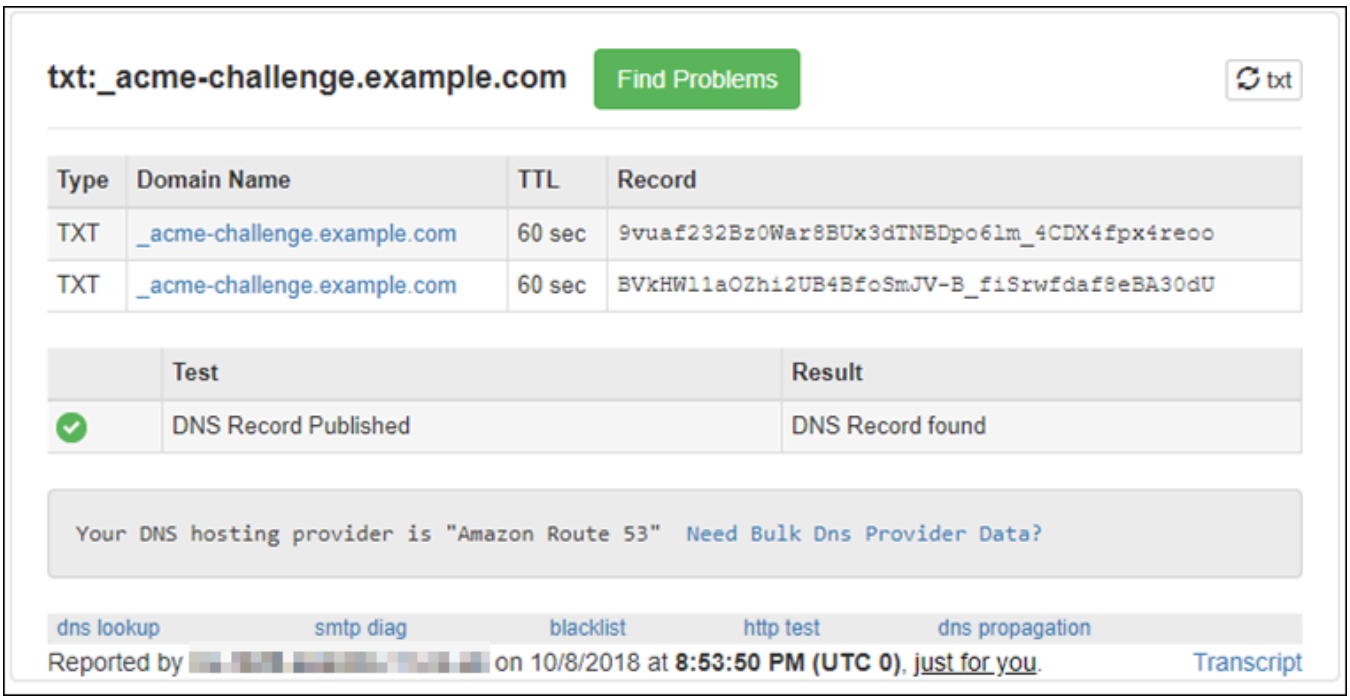
   Beispiel:

   ```
   _acme-challenge.example.com
   ```

3. Wählen Sie TXT Lookup (TXT-Suche), um die Prüfung auszuführen.
4. Eine der folgenden Antworten wird eintreten:

   - Wenn Ihre TXT-Datensätze an das DNS des Internets weitergegeben wurden, sehen Sie eine ähnliche Antwort wie im folgenden Screenshot. Schließen Sie das Browserfenster und fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.



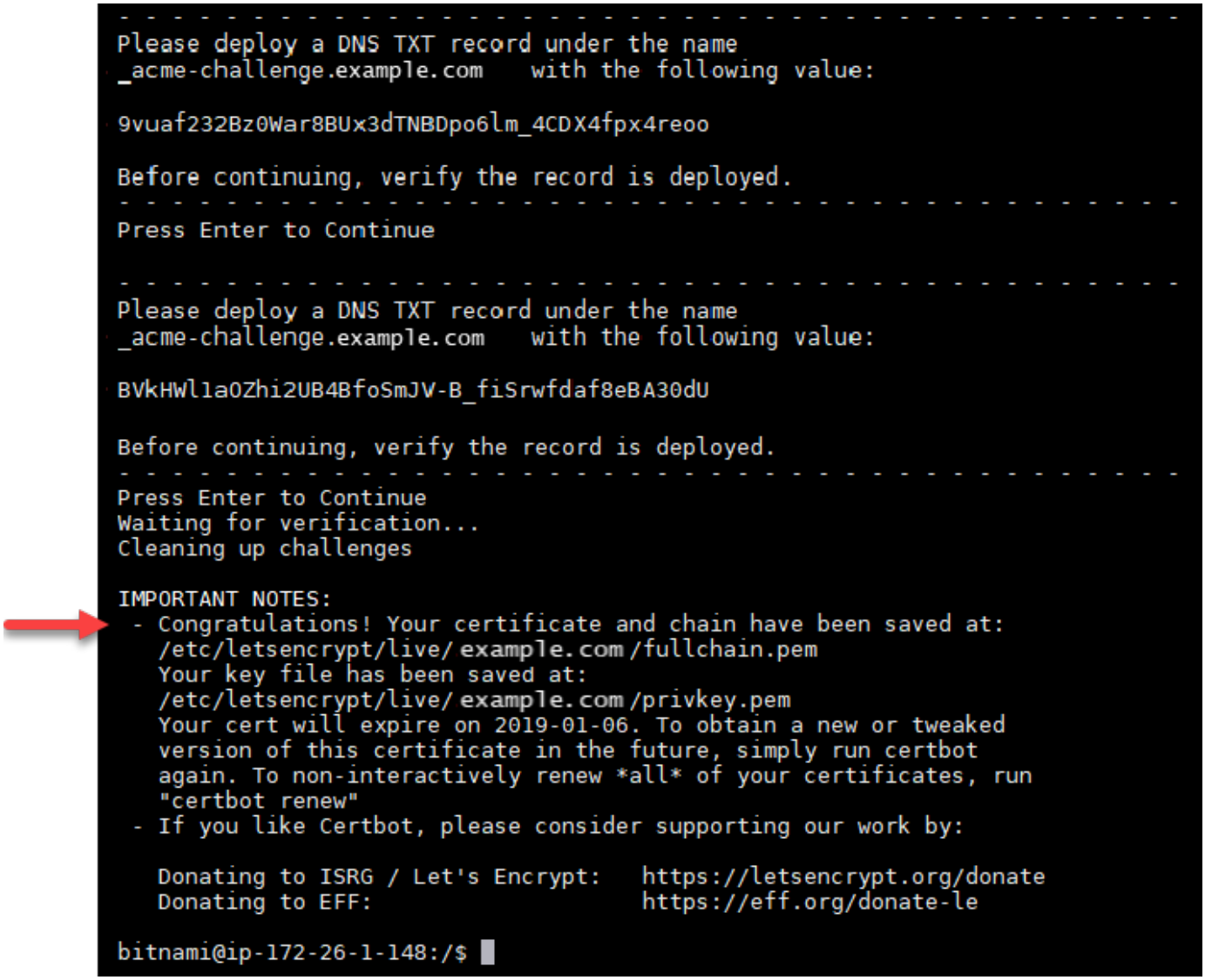
- Wenn Ihre TXT-Einträge nicht über das DNS des Internets verbreitet wurden, sehen Sie eine Antwort wie DNS Record not found (DNS-Datensatz nicht gefunden). Vergewissern Sie sich, dass Sie die richtigen DNS-Einträge zur DNS-Zone Ihrer Domäne hinzugefügt haben. Wenn Sie die richtigen Datensätze hinzugefügt haben, warten Sie noch eine Weile, bis sich die DNS-Einträge Ihrer Domäne verbreiten, und führen Sie die TXT-Suche erneut aus.

Schritt 6: Abschließen der Let's Encrypt SSL-Zertifikatsanforderung

Kehren Sie zur browserbasierten Lightsail-SSH-Sitzung für Ihre WordPress Instanz zurück und schließen Sie die Let's Encrypt-Zertifikatsanforderung ab. Certbot speichert Ihr SSL-Zertifikat, Ihre Kette und Ihre Schlüsseldateien in einem bestimmten Verzeichnis auf Ihrer Instanz. WordPress

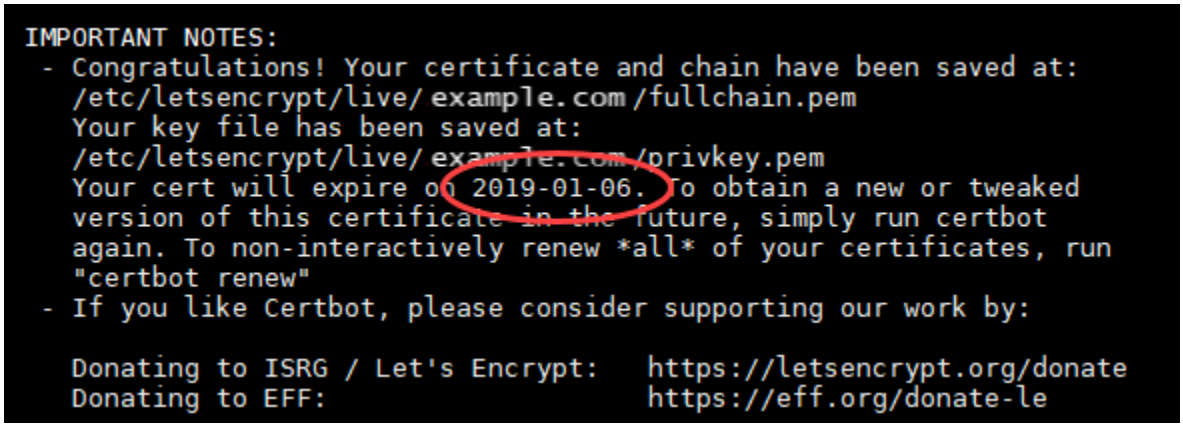
So schließen Sie die Let's Encrypt SSL-Zertifikatsanforderung ab

1. Drücken Sie in der browserbasierten Lightsail-SSH-Sitzung für Ihre WordPress Instance die Eingabetaste, um mit Ihrer Let's Encrypt SSL-Zertifikatsanfrage fortzufahren. Bei Erfolg erscheint eine Antwort ähnlich der im folgenden Screenshot:



Die Nachricht bestätigt, dass Ihre Zertifikats-, Ketten- und Schlüsseldateien im Verzeichnis `/etc/letsencrypt/live/`*`domain`*`/` gespeichert sind. Stellen Sie sicher, dass Sie *`domain`* durch Ihre Domäne ersetzen, wie z. B. `/etc/letsencrypt/live/`*`example.com`*`/`.

2. Notieren Sie sich das in der Nachricht angegebene Ablaufdatum. Sie verwenden es, um Ihr Zertifikat bis zu diesem Datum zu verlängern.



3. Da Sie nun das Let's Encrypt SSL-Zertifikat haben, fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 7: Erstellen von Links zu den Let's Encrypt-Zertifikatsdateien im Apache-Serververzeichnis

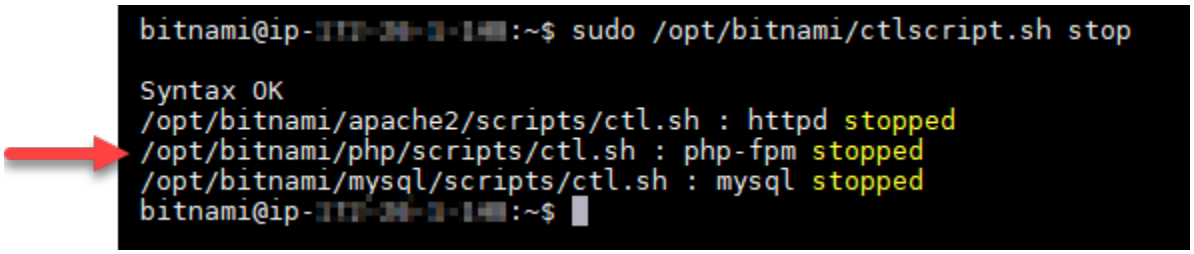
Erstellen Sie Links zu den Let's Encrypt SSL-Zertifikatsdateien im Apache-Serververzeichnis auf Ihrer Instanz. WordPress Außerdem sichern Sie Ihre vorhandenen Zertifikate, falls Sie sie später benötigen.

So erstellen Sie Links zu den Let's Encrypt-Zertifikatsdateien im Apache-Server-Verzeichnis

1. Geben Sie in der browserbasierten Lightsail-SSH-Sitzung für Ihre WordPress Instanz den folgenden Befehl ein, um die zugrunde liegenden Dienste zu beenden:

   ```
   sudo /opt/bitnami/ctlscript.sh stop
   ```

   Es wird eine Antwort ähnlich der folgenden angezeigt:

2. Geben Sie den folgenden Befehl ein, um eine Umgebungsvariable für Ihre Domäne zu setzen. Sie können die Befehle effizienter kopieren und einfügen, um Ihre Zertifikatdateien zu verknüpfen. Achten Sie darauf, *domain* durch Ihren registrierten Domänennamen zu ersetzen.

```
DOMAIN=domain
```

Beispiel:

```
DOMAIN=example.com
```

3. Geben Sie den folgenden Befehl ein, um zu bestätigen, dass die Variablen die richtigen Werte zurückgeben:

```
echo $DOMAIN
```

Das Ergebnis sollte in etwa wie folgt aussehen:

4. Geben Sie die folgenden Befehle einzeln ein, um Ihre vorhandenen Zertifikatsdateien als Backups umzubenennen. Informationen zu den verschiedenen Verteilungen und Dateistrukturen finden Sie im Abschnitt Wichtig am Anfang dieses Tutorials.

   - Für Debian-Linux-Verteilungen

     Ansatz A (Bitnami-Installationen mit Systempaketen):

     ```
     sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.crt /opt/bitnami/apache2/
     conf/bitnami/certs/server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.key /opt/bitnami/apache2/
     conf/bitnami/certs/server.key.old
     ```

     Ansatz B (Eigenständige Bitnami-Installationen):

     ```
     sudo mv /opt/bitnami/apache2/conf/server.crt /opt/bitnami/apache2/conf/
     server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/apache2/conf/server.key /opt/bitnami/apache2/conf/
     server.key.old
     ```

- Für ältere Instances, die die Ubuntu-Linux-Verteilung verwenden:

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.crt /opt/bitnami/apache/
conf/bitnami/certs/server.crt.old
```

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.key /opt/bitnami/apache/
conf/bitnami/certs/server.key.old
```

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.csr /opt/bitnami/apache/
conf/bitnami/certs/server.csr.old
```

5. Geben Sie die folgenden Befehle einzeln ein, um Links zu Ihren Zertifikatsdateien von Let's Encrypt im Apache-Verzeichnis zu erstellen. Informationen zu den verschiedenen Verteilungen und Dateistrukturen finden Sie im Abschnitt Wichtig am Anfang dieses Tutorials.

   - Für Debian-Linux-Verteilungen

     Ansatz A (Bitnami-Installationen mit Systempaketen):

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/
     bitnami/certs/server.key
     ```

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/
     conf/bitnami/certs/server.crt
     ```

     Ansatz B (Eigenständige Bitnami-Installationen):

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/
     server.key
     ```

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/
     conf/server.crt
     ```

   - Für ältere Instances, die die Ubuntu-Linux-Verteilung verwenden:

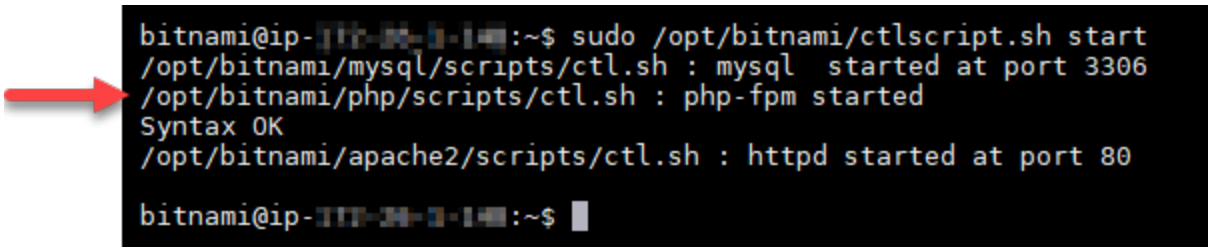
     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache/conf/
     bitnami/certs/server.key
     ```

```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache/conf/
bitnami/certs/server.crt
```

6. Geben Sie den folgenden Befehl ein, um die zugrunde liegenden Services zu starten, die Sie zuvor gestoppt haben:

   ```
   sudo /opt/bitnami/ctlscript.sh start
   ```

   Das Ergebnis sollte in etwa wie folgt aussehen:

   Die SSL-Zertifikatsdateien für Ihre WordPress Instanz befinden sich jetzt im richtigen Verzeichnis.

7. Fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort.

Schritt 8: Integrieren Sie das SSL-Zertifikat mithilfe des Really Simple SSL-Plug-ins in Ihre WordPress Site

Installieren Sie das Really Simple SSL-Plug-In auf Ihrer WordPress Website und verwenden Sie es, um das SSL-Zertifikat zu integrieren. Really Simple SSL konfiguriert auch die HTTP zu HTTPS-Weiterleitung, um sicherzustellen, dass Benutzer, die Ihre Website besuchen, sich immer auf der HTTPS-Verbindung befinden.

Um das SSL-Zertifikat mithilfe des Really Simple SSL-Plug-ins in Ihre WordPress Website zu integrieren

1. Geben Sie in der browserbasierten Lightsail-SSH-Sitzung für Ihre WordPress Instanz den folgenden Befehl ein, um Ihre `htaccess.conf` Dateien als schreibbar `wp-config.php` festzulegen. Das Really-Simple-SSL-Plug-In schreibt in die Datei wp-config.php, um Ihre Zertifikate zu konfigurieren.

   - Für neuere Instances, die die Debian-Linux-Verteilung verwenden:

```
sudo chmod 666 /opt/bitnami/wordpress/wp-config.php && sudo chmod 666 /opt/
bitnami/apache/conf/vhosts/htaccess/wordpress-htaccess.conf
```

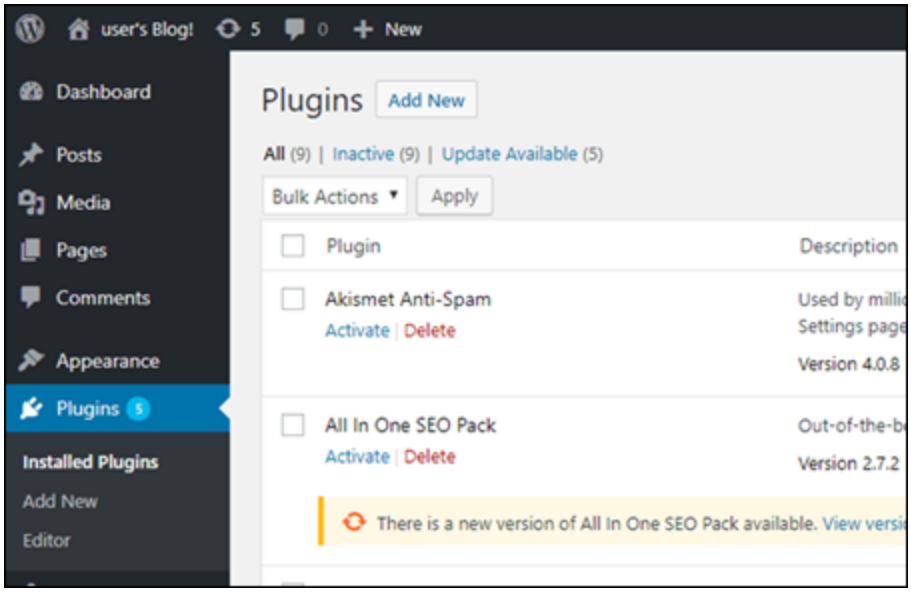
- Für ältere Instances, die die Ubuntu-Linux-Verteilung verwenden:

```
sudo chmod 666 /opt/bitnami/apps/wordpress/htdocs/wp-config.php && sudo chmod
 666 /opt/bitnami/apps/wordpress/conf/htaccess.conf
```

2. Öffnen Sie ein neues Browserfenster und melden Sie sich im Administrations-Dashboard Ihrer Instanz an. WordPress

> **Note**
>
> Weitere Informationen finden Sie unter Abrufen des Anwendungsbenutzernamens und des Kennworts für Ihre Bitnami-Instance in Amazon Lightsail.

3. Wählen Sie im linken Navigationsbereich Plugins aus.
4. Wählen Sie oben auf der Plugin-Seite Add New (Neu hinzufügen).



5. Suchen Sie nach Really Simple SSL.
6. Wählen Sie Install Now (Jetzt installieren) neben dem Really-Simple-SSL-Plug-in in den Suchergebnissen.

7. Nachdem die Installation abgeschlossen ist, klicken Sie auf Activate (Aktivieren).
8. Wählen Sie in der angezeigten Eingabeaufforderung Go ahead, activate SSL! (Los, aktivieren Sie SSL!) Möglicherweise werden Sie zur Anmeldeseite für das Administrations-Dashboard Ihrer WordPress Instanz weitergeleitet.

   Ihre WordPress Instance ist jetzt für die Verwendung der SSL-Verschlüsselung konfiguriert. Darüber hinaus ist Ihre WordPress Instance jetzt so konfiguriert, dass Verbindungen automatisch von HTTP zu HTTPS umgeleitet werden. Wenn ein Besucher zu `http://example.com` geht, wird er automatisch an die verschlüsselte HTTPS-Verbindung weitergeleitet (z. B.: `https://example.com`).

Schritt 9: Erneuern der Let's Encrypt Zertifikate alle 90 Tage

Die Zertifikate von Let's Encrypt sind 90 Tage lang gültig. Die Zertifikate können 30 Tage bevor sie ablaufen erneuert werden. Um die Let's Encrypt-Zertifikate zu erneuern, führen Sie den ursprünglichen Befehl aus, mit dem sie abgerufen wurden. Wiederholen Sie die Schritte im Abschnitt Anfordern eines Let's Encrypt SSL-Wildcard-Zertifikats in diesem Tutorial.

Netzwerk-Tutorials für Amazon Lightsail

In den folgenden Netzwerk-Tutorials erfahren Sie mehr über Lightsail-verwandte Themen wie die Einrichtung von Amazon-VPC-Peering und die Konfiguration von Reverse-DNS.

Themen

- Konfigurieren von IPv6 auf cPanel-Instances in Lightsail
- Konfigurieren von IPv6 auf Debian-8-Instances in Lightsail
- Konfigurieren von IPv6 für GitLab Instances in Lightsail

- Konfigurieren von IPv6 auf Nginx-Instances in Lightsail
- Konfigurieren von IPv6 auf Plesk-Instances in Lightsail
- Konfigurieren von IPv6 für Ubuntu-16-Instances in Lightsail

Konfigurieren von IPv6 auf cPanel-Instances in Lightsail

Allen Instances in Amazon Lightsail sind standardmäßig eine öffentliche und eine private IPv4-Adresse zugewiesen. Optional können Sie IPv6 aktivieren, damit Ihren Instance eine öffentliche IPv6-Adresse zugewiesen wird. Weitere Informationen finden Sie unter Amazon Lightsail-IP-Adressen und Aktivieren oder Deaktivieren von IPv6.

Nachdem Sie IPv6 für eine Instance aktiviert haben, die den cPanel & WHM-Blueprint verwendet, müssen Sie weitere Schritte ausführen, um die Instance auf ihre IPv6-Adresse aufmerksam zu machen. In diesem Leitfaden zeigen wir Ihnen die zusätzlichen Schritte, die Sie für cPanel & WHM-Instance ausführen müssen.

Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies noch nicht geschehen ist:

- Erstellen Sie eine cPanel & WHM-Instance in Lightsail. Weitere Informationen finden Sie unter Erstellen einer Instance.
- Konfigurieren Sie Ihre cPanel & WHM-Instance. Weitere Informationen finden Sie im Schnellstarthandbuch: cPanel & WHM auf Amazon Lightsail.

> **Important**
>
> Stellen Sie sicher, dass alle Softwareupdates und erforderlichen Systemneustarts durchgeführt werden, bevor Sie mit den Schritten in diesem Leitfaden fortfahren.

- Aktivieren Sie IPv6 für Ihre cPanel & WHM-Instance. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren von IPv6.

> **Note**
>
> Neue cPanel & WHM-Instances, die am oder nach dem 12. Januar 2021 erstellt wurden, haben IPv6 standardmäßig aktiviert, wenn sie in der Lightsail -Konsole erstellt werden. Sie

müssen die folgenden Schritte in diesem Leitfaden ausführen, um IPv6 für Ihre Instance zu konfigurieren, selbst wenn IPv6 beim Erstellen der Instance standardmäßig aktiviert war.

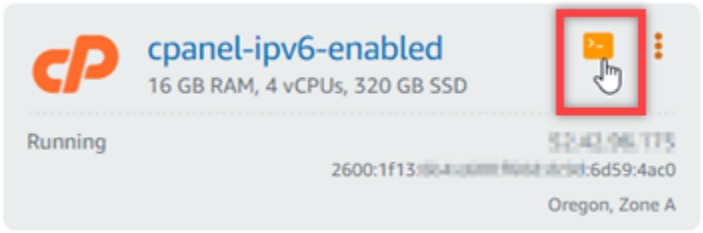
Konfigurieren von IPv6 für eine GitLab-Instance

Führen Sie das folgende Verfahren aus, um IPv6 auf einer cPanel & WHM-Instance in Lightsail zu konfigurieren.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. **Important**

   Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um SSH oder RDP über IPv6 in Ihre Instance zu übertragen. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

   Suchen Sie im Abschnitt Instances der Lightsail-Startseite die cPanel & WHM-Instance, die Sie konfigurieren möchten, und wählen Sie das browserbasierte SSH-Client-Symbol aus, um über SSH eine Verbindung zu ihr herzustellen.

3. Nachdem Sie mit Ihrer Instance verbunden sind, geben Sie den folgenden Befehl ein, um die `ifcfg-eth0`-Netzwerkschnittstellen-Konfigurationsdatei mit Nano zu öffnen.

   ```
   sudo nano /etc/sysconfig/network-scripts/ifcfg-eth0
   ```

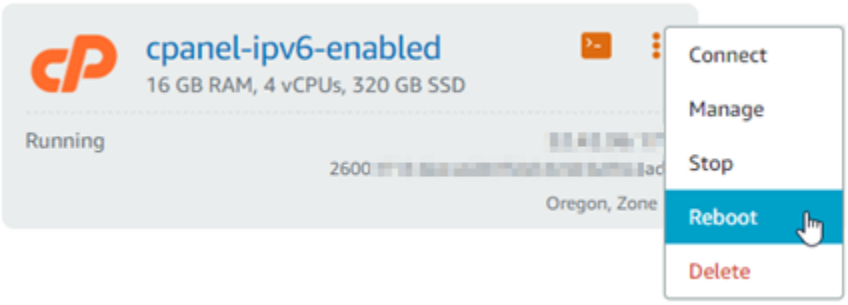
4. Fügen Sie der Datei die folgenden Textzeilen hinzu, wenn sie noch nicht vorhanden sind.

   ```
   IPV6INIT=yes
   IPV6_AUTOCONF=yes
   DHCPV6C=yes
   ```

Das Ergebnis sollte wie folgt aussehen:

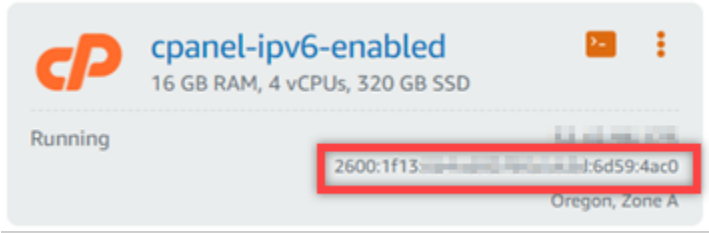
```
# Automatically generated by the vm import process
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=eth0
DEVICE=eth0
ONBOOT=yes
IPV6INIT=yes
IPV6_FAILURE_FATAL=no
DHCPV6C=yes
IPV6_AUTOCONF=yes
```

5. Drücken Sie auf STRG+C auf Ihrer Tastatur, um die Datei zu verlassen.
6. Drücken Sie auf Y, wenn Sie aufgefordert werden, den geänderten Puffer zu speichern, und drücken Sie Enter, um in der vorhandenen Datei zu speichern. Dadurch werden die Änderungen gespeichert, die Sie in der `ifcfg-eth0`-Netzwerkschnittstellen-Konfigurationsdatei vorgenommen haben.
7. Schließen Sie das browserbasierte SSH-Fenster und wechseln Sie zurück zur Lightsail-Konsole.
8. In der Registerkarte Instances der Lightsail-Startseite wählen Sie das Aktionsmenü (⋮) für die cPanel & WHM-Instance und wählen Sie Neustart aus.

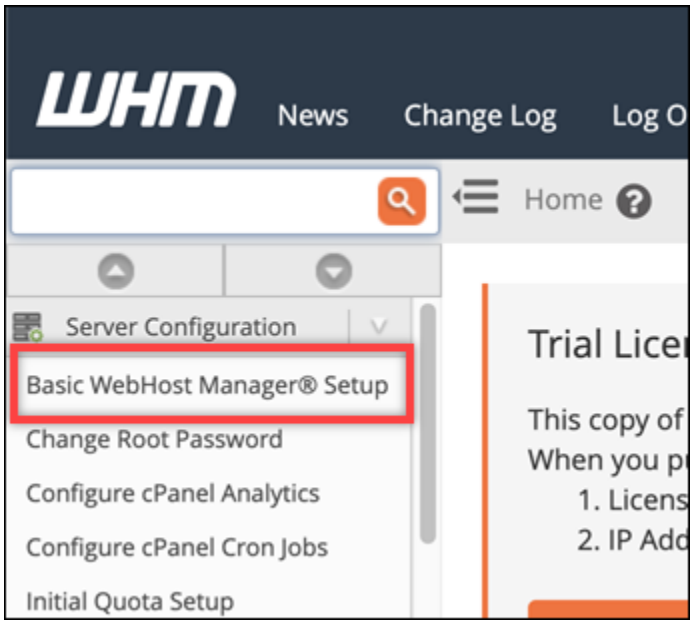


Warten Sie einige Minuten, bis Ihre Instance neu gestartet wird, bevor Sie mit dem nächsten Schritt fortfahren.

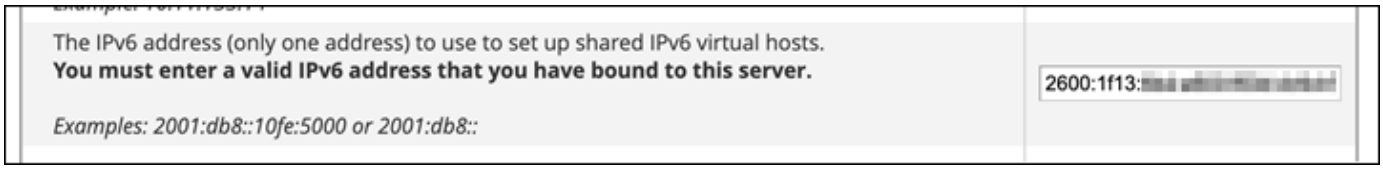
9. In der Registerkarte Instances der Lightsail-Startseite, notieren Sie sich die IPv6-Adresse, die Ihrer cPanel & WHM-Instance zugewiesen ist.



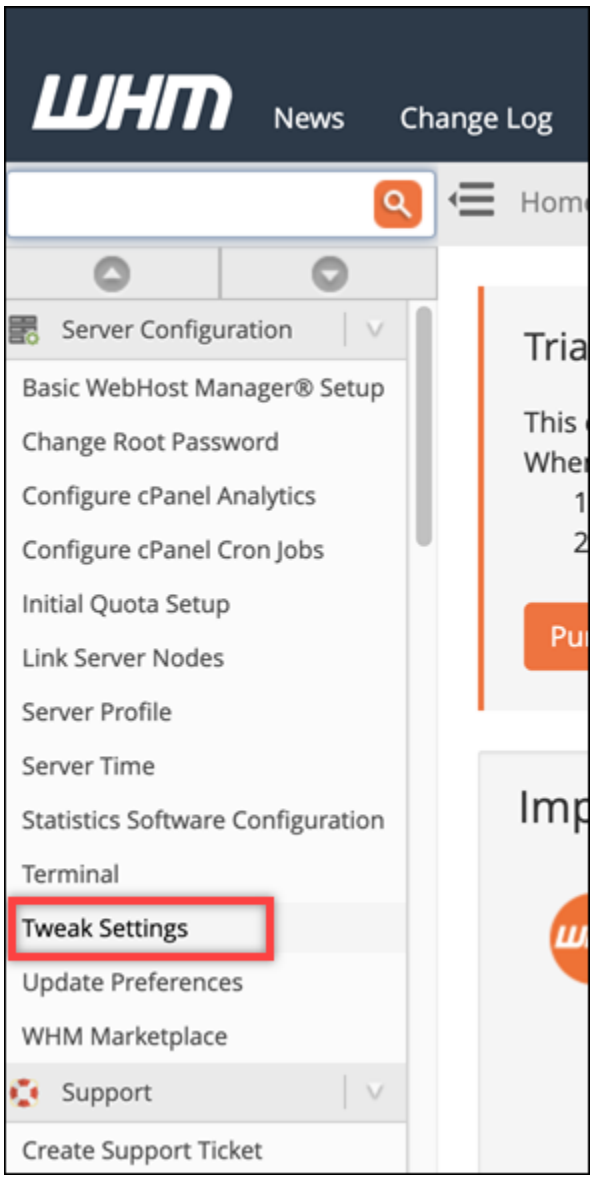
10. Öffnen Sie eine neue Browser-Registerkarte und melden Sie sich beim Web Host Manager (WHM) Ihrer cPanel & WHM-Instance an.
11. Wählen Sie im linken Navigationsbereich der WHM-Konsole Basic WebHost Manager Setup aus.



12. In der Registerkarte Alle suchen Sie den Text für Zu verwendende IPv6-Adresse und geben Sie dann die IPv6-Adresse ein, die Ihrer Instance zugewiesen ist. Sie sollten sich die IPv6-Adresse notieren, die Ihrer Instance aus Schritt 9 dieses Verfahrens zugewiesen wurde.

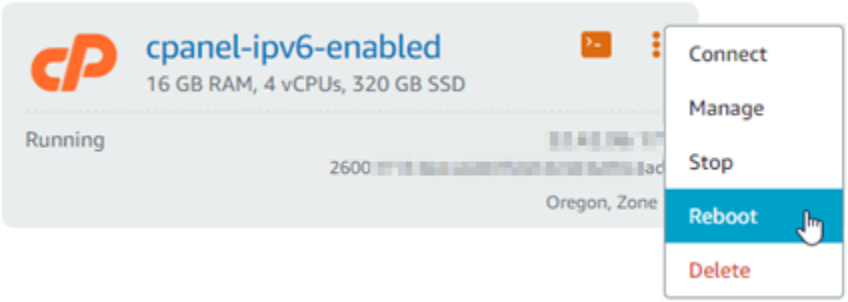


13. Scrollen Sie auf der Seite nach unten und wählen Sie Änderungen Speichern.
14. Wählen Sie im linken Navigationsbereich der WHM Konsole Tweak Settings.



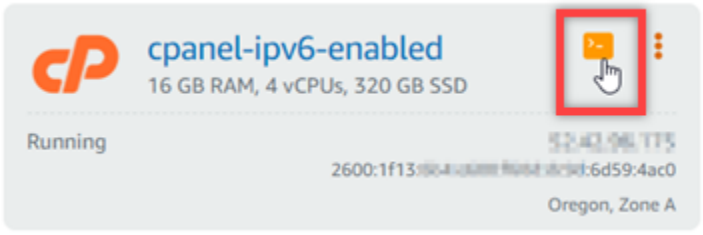
15. Scrollen Sie in der Registerkarte Alle nach unten, um die IPv6-Adressen anhören und stellen Sie sie auf On.

16. Scrollen Sie auf der Seite nach unten und wählen Sie Speichern.
17. Wechseln Sie zurück zur Lightsail-Konsole.
18. In der Registerkarte Instances der Lightsail-Startseite wählen Sie das Aktionsmenü (⋮) für die cPanel & WHM-Instance und wählen Sie Neustart aus.



Warten Sie einige Minuten, bis Ihre Instance neu gestartet wird, bevor Sie mit dem nächsten Schritt fortfahren.

19. Wählen Sie das browserbasierte SSH-Client-Symbol für die cPanel & WHM-Instance aus, um mit SSH eine Verbindung herzustellen.



20. Nachdem Sie eine Verbindung mit der Instance hergestellt haben, geben Sie den folgenden Befehl ein, um die für Ihre Instance konfigurierten IP-Adressen anzuzeigen und zu bestätigen, dass sie nun die zugewiesene IPv6-Adresse erkennt.

```
ip addr
```

Es wird eine Antwort ähnlich dem folgenden Beispiel angezeigt. Wenn Ihre Instance ihre IPv6-Adresse erkennt, wird sie in der Antwort mit der Bezeichnung scope global angezeigt, wie in diesem Beispiel sichtbar.

```
[centos@ ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 02:9b:51:92:50:45 brd ff:ff:ff:ff:ff:ff
    inet /20 brd  scope global dynamic eth0
    inet6 2600:1f13:  :6d59:4ac0/128 scope global dynamic
    inet6 fe80:  :5045/64 scope link
       valid_lft forever preferred_lft forever
```

21. Geben Sie den folgenden Befehl ein, um zu bestätigen, dass Ihre Instance eine IPv6-Adresse pingen kann.

```
ping6 ipv6.google.com -c 6
```

Das Ergebnis sollte wie das folgende Beispiel aussehen, das bestätigt, dass Ihre Instance IPv6-Adressen pingen kann.

Konfigurieren von IPv6 auf Debian-8-Instances in Lightsail

Allen Instances in Amazon Lightsail sind standardmäßig eine öffentliche und eine private IPv4-Adresse zugewiesen. Optional können Sie IPv6 aktivieren, damit Ihren Instance eine öffentliche IPv6-Adresse zugewiesen wird. Weitere Informationen finden Sie unter Amazon Lightsail-IP-Adressen und Aktivieren oder Deaktivieren von IPv6.

Nachdem Sie IPv6 für eine Instance aktiviert haben, die den Debian-8-Blueprint verwendet, müssen Sie zusätzliche Schritte ausführen, um die Instanz auf ihre IPv6-Adresse aufmerksam zu machen. In dieser Anleitung zeigen wir Ihnen die zusätzlichen Schritte, die Sie für Debian-8-Instances ausführen müssen.

Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies noch nicht geschehen ist:

- Erstellen Sie eine Debian-8-Instance in Lightsail. Weitere Informationen finden Sie unter Erstellen einer Instance.

- Aktivieren Sie IPv6 für Ihre Debian-8-Instance. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren von IPv6.

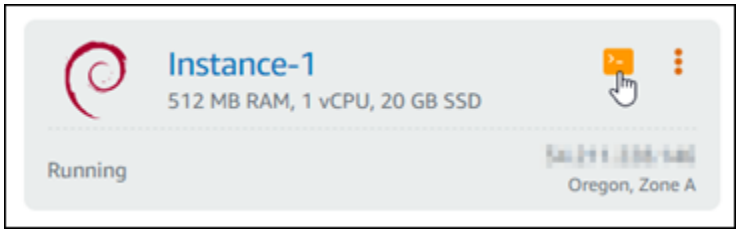
> **Note**
>
> Neue Debian-Instances , die am oder nach dem 12. Januar 2021 erstellt wurden, haben IPv6 standardmäßig aktiviert, wenn sie in der Lightsail-Konsole erstellt werden. Sie müssen die folgenden Schritte in diesem Handbuch ausführen, um IPv6 für Ihre Instance zu konfigurieren, selbst wenn IPv6 beim Erstellen der Instance standardmäßig aktiviert war.

Konfigurieren von IPv6 auf einer Debian-8-Instance

Führen Sie das folgende Verfahren aus, um IPv6 auf einer Debian-8-Instance in Lightsail zu konfigurieren.

1. Melden Sie sich bei der Lightsail-Konsole an.
2.
> **Important**
>
> Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um über IPv6 SSH oder RDP in Ihre Instance zu senden. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

   Suchen Sie im Abschnitt Instances der Lightsail-Startseite die Debian-8-Instance, die Sie konfigurieren möchten, und wählen Sie das browserbasierte SSH-Client-Symbol aus, um über SSH eine Verbindung zu ihr herzustellen.

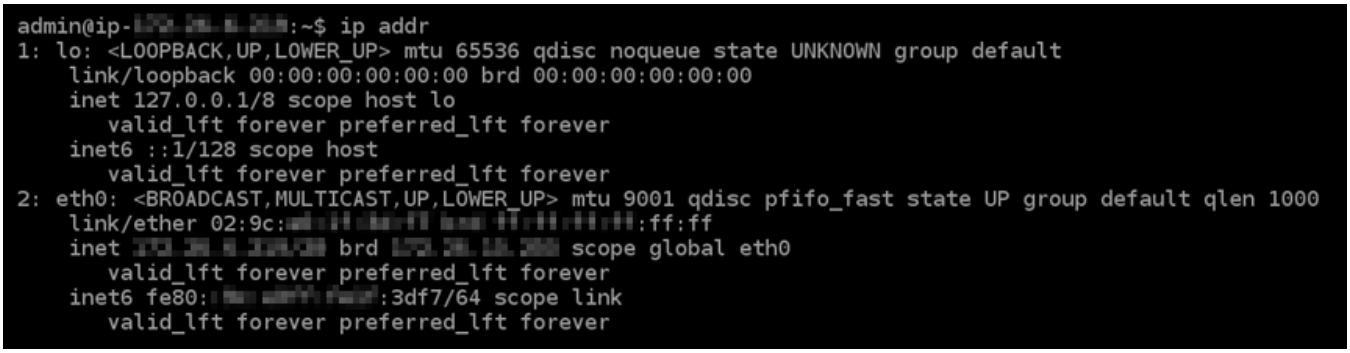


3. Nachdem Sie eine Verbindung mit der Instance hergestellt haben, geben Sie den folgenden Befehl ein, um die für Ihre Instance konfigurierten IP-Adressen anzuzeigen.

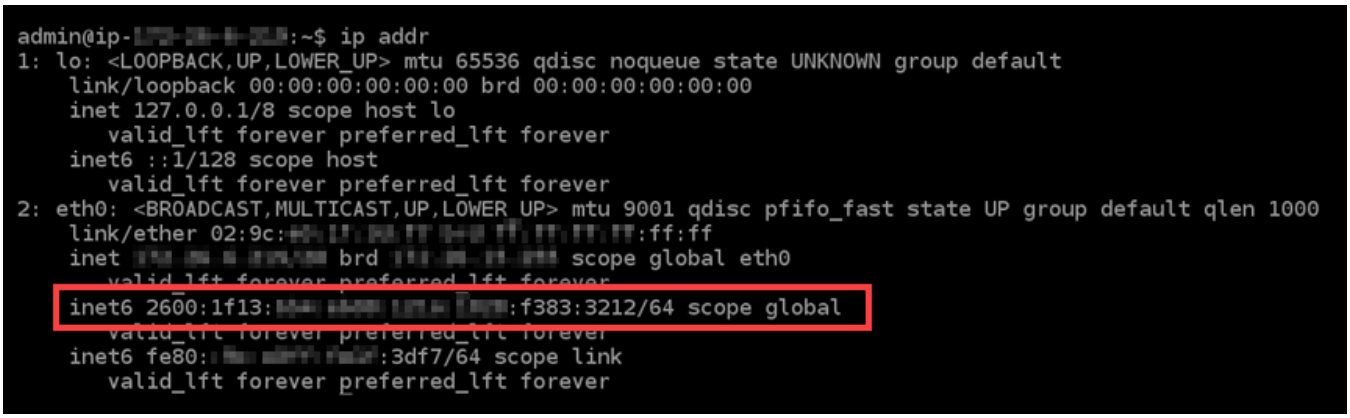
```
ip addr
```

Es wird eine Antwort ähnlich dem folgenden Beispiel angezeigt:

- Wenn Ihre Instance ihre IPv6-Adresse nicht erkennt, wird sie in der Antwort nicht aufgeführt. Sie sollten die Schritte 4 bis 9 dieses Verfahrens fortsetzen.



- Wenn Ihre Instance ihre IPv6-Adresse erkennt, wird sie in der Antwort mit einem `scope global`, wie in diesem Beispiel gezeigt. Sie sollten hier anhalten. Sie müssen die Schritte 4 bis 9 dieses Verfahrens nicht ausführen, da Ihre Instance bereits so konfiguriert ist, dass sie ihre IPv6-Adresse erkennt.



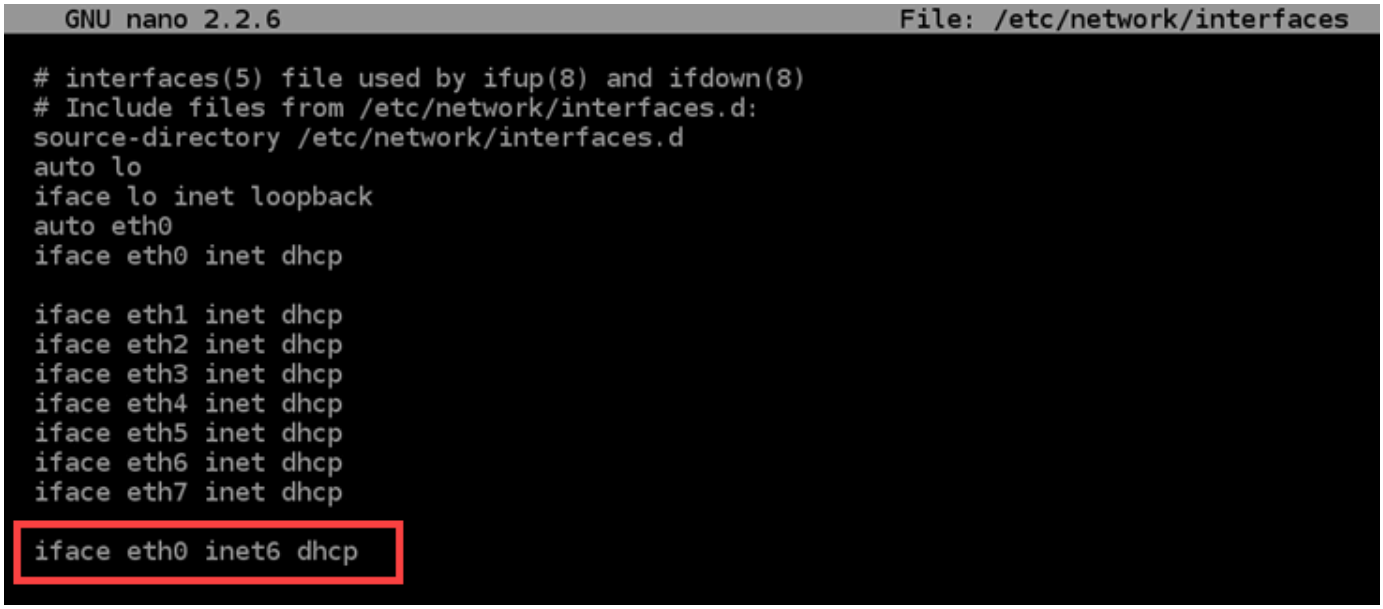
4. Geben Sie den folgenden Befehl ein, um die`interfaces`-Konfigurationsdatei mit Nano zu öffnen.

```
sudo nano /etc/network/interfaces
```

5. Fügen Sie die folgende Zeile am Ende der Datei hinzu.

```
iface eth0 inet6 dhcp
```

Wenn Sie fertig sind, sieht die Datei wie folgt aus:



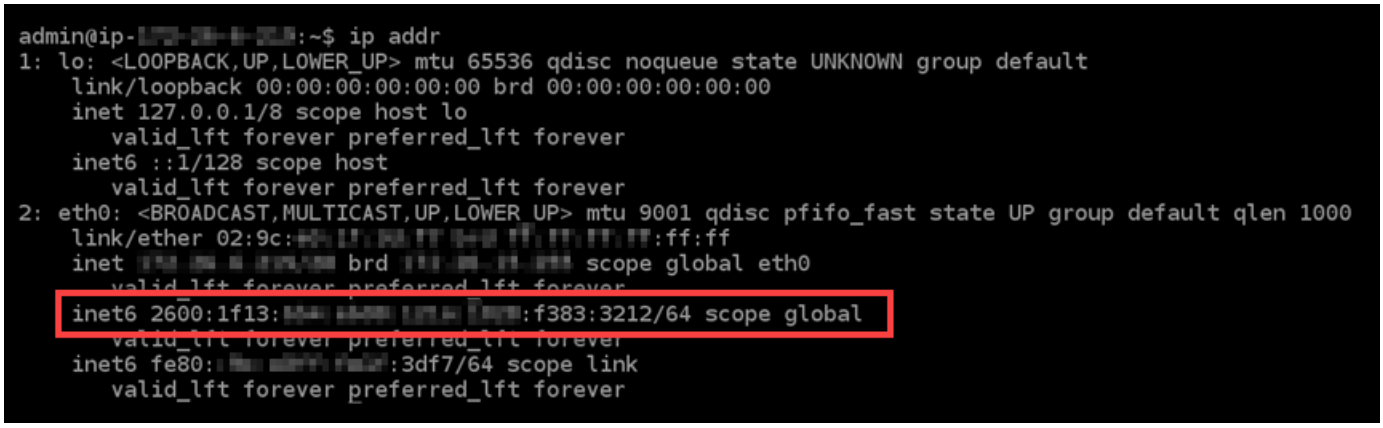
6. Drücken Sie die Strg+Esc, um Nano zu verlassen.
7. Drücken Sie Y, wenn Sie gefragt werden, ob Sie den geänderten Puffer speichern möchten, drücken Sie die Eingabetaste, um in der vorhandenen Schnittstellen-Konfigurationsdatei zu speichern.
8. Geben Sie den folgenden Befehl ein, um die Services auf der Instance neu zu starten.

   ```
   sudo systemctl restart networking
   ```

   Möglicherweise müssen Sie noch einige Minuten warten, damit Ihre Instance ihre IPv6-Adresse erkennt, nachdem Sie den Netzwerkdienst Ihrer Instance neu gestartet haben.
9. Geben Sie den folgenden Befehl ein, um die für Ihre Instance konfigurierten IP-Adressen anzuzeigen, und bestätigen Sie, dass die zugewiesene IPv6-Adresse jetzt erkannt wird.

   ```
   ip addr
   ```

   Es wird eine Antwort ähnlich dem folgenden Beispiel angezeigt. Wenn Ihre Instance ihre IPv6-Adresse erkennt, wird sie in der Antwort mit der Bezeichnung `scope global` wie in diesem Beispiel gezeigt.



Konfigurieren von IPv6 für GitLab Instances in Lightsail

Allen Instances in Amazon Lightsail sind standardmäßig eine öffentliche und eine private IPv4-Adresse zugewiesen. Optional können Sie IPv6 aktivieren, damit Ihren Instance eine öffentliche IPv6-Adresse zugewiesen wird. Weitere Informationen finden Sie unter Amazon Lightsail-IP-Adressen und Aktivieren oder Deaktivieren von IPv6.

Nachdem Sie IPv6 für eine Instance aktiviert haben, die den GitLab Blueprint verwendet, müssen Sie zusätzliche Schritte ausführen, um die Instance auf ihre IPv6-Adresse aufmerksam zu machen. In diesem Leitfaden zeigen wir Ihnen die zusätzlichen Schritte, die Sie für GitLab Instances ausführen müssen.

Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies noch nicht geschehen ist:

- Erstellen Sie eine GitLab Instance in Lightsail. Weitere Informationen finden Sie unter Erstellen einer Instance.
- Aktivieren Sie IPv6 für Ihre GitLab Instance. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren von IPv6.

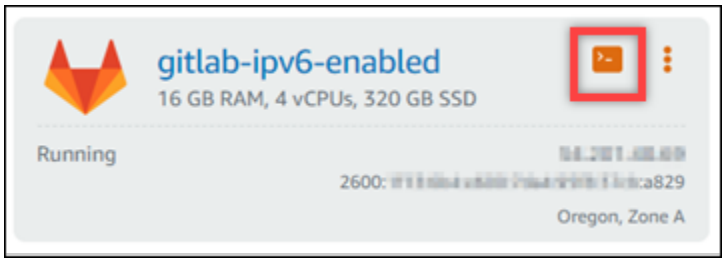
> **Note**
>
> Für neue GitLab Instances, die am oder nach dem 12. Januar 2021 erstellt wurden, ist IPv6 standardmäßig aktiviert, wenn sie in der Lightsail-Konsole erstellt werden. Sie müssen die folgenden Schritte in diesem Handbuch ausführen, um IPv6 für Ihre Instance zu konfigurieren, selbst wenn IPv6 beim Erstellen der Instance standardmäßig aktiviert war.

Konfigurieren von IPv6 auf einer GitLab Instance

Führen Sie das folgende Verfahren aus, um IPv6 auf einer GitLab Instance in Lightsail zu konfigurieren.

1. Melden Sie sich bei der Lightsail-Konsole an.
2.
> **Important**
>
> Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um SSH oder RDP über IPv6 in Ihre Instance zu übertragen. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

   Suchen Sie im Abschnitt Instances der Lightsail-Startseite die GitLab Instance, die Sie konfigurieren möchten, und wählen Sie das browserbasierte SSH-Client-Symbol aus, um über SSH eine Verbindung zu ihr herzustellen.



3. Nachdem Sie eine Verbindung mit der Instance hergestellt haben, geben Sie den folgenden Befehl ein, um die für Ihre Instance konfigurierten IP-Adressen anzuzeigen.

```
ip addr
```

   Es wird eine Antwort ähnlich dem folgenden Beispiel angezeigt:

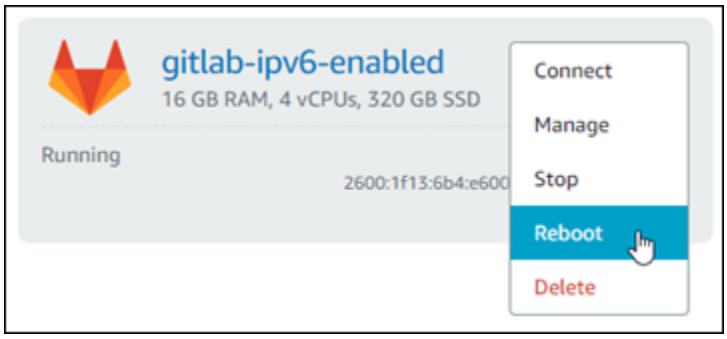
   - Wenn Ihre Instance ihre IPv6-Adresse nicht erkennt, wird sie in der Antwort nicht aufgeführt. Sie sollten die Schritte 4 bis 9 dieses Verfahrens fortsetzen.

```
admin@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80:[redacted]:3df7/64 scope link
       valid_lft forever preferred_lft forever
```

- Wenn Ihre Instance ihre IPv6-Adresse erkennt, wird sie in der Antwort mit einem `scope global`, wie in diesem Beispiel gezeigt. Sie sollten hier anhalten. Sie müssen die Schritte 4 bis 9 dieses Verfahrens nicht ausführen, da Ihre Instance bereits so konfiguriert ist, dass sie ihre IPv6-Adresse erkennt.

```
admin@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2600:1f13:[redacted]:f383:3212/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80:[redacted]:3df7/64 scope link
       valid_lft forever preferred_lft forever
```

4. Wechseln Sie zurück zur Lightsail-Konsole.
5. Wählen Sie auf der Registerkarte Instances der Lightsail-Startseite das Aktionsmenü (⋮) für die GitLab Instance und dann Neustart aus.



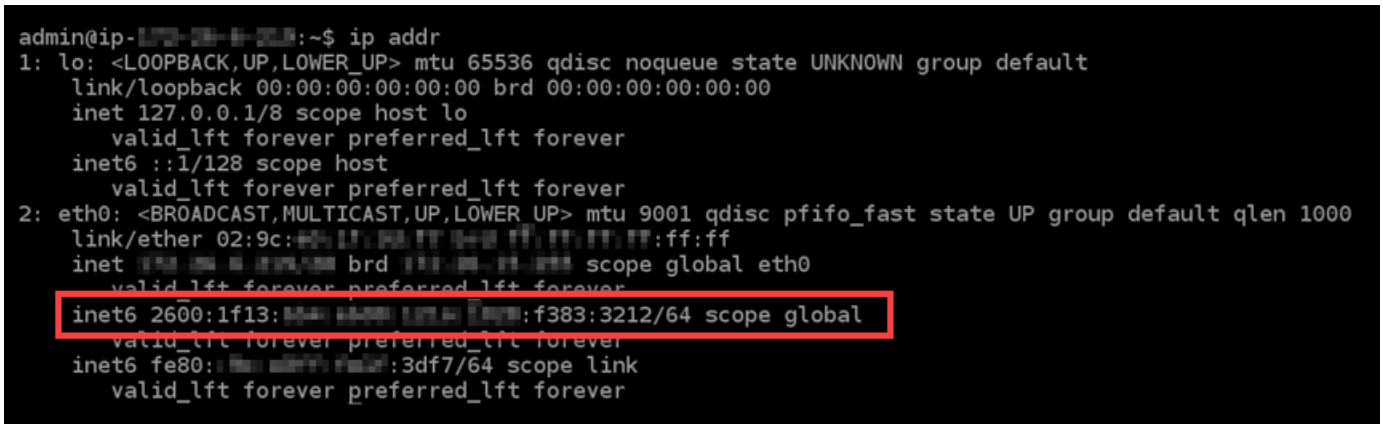
Warten Sie einige Minuten, bis Ihre Instance neu gestartet wird, bevor Sie mit dem nächsten Schritt fortfahren.

6. Wechseln Sie zurück zur SSH-Sitzung Ihrer GitLab Instance.

7. Geben Sie den folgenden Befehl ein, um die für Ihre Instance konfigurierten IP-Adressen anzuzeigen, und bestätigen Sie, dass die zugewiesene IPv6-Adresse jetzt erkannt wird.

```
ip addr
```

Es wird eine Antwort ähnlich dem folgenden Beispiel angezeigt. Wenn Ihre Instance ihre IPv6-Adresse erkennt, wird sie in der Antwort mit der Bezeichnung `scope global`, wie in diesem Beispiel gezeigt.



Konfigurieren von IPv6 auf Nginx-Instances in Lightsail

Allen Instances in Amazon Lightsail sind standardmäßig eine öffentliche und eine private IPv4-Adresse zugewiesen. Optional können Sie IPv6 aktivieren, damit Ihren Instance eine öffentliche IPv6-Adresse zugewiesen wird. Weitere Informationen finden Sie unter Amazon Lightsail-IP-Adressen und Aktivieren oder Deaktivieren von IPv6.

Nachdem Sie IPv6 für eine Instance aktiviert haben, die den Nginx-Blueprint verwendet, müssen Sie weitere Schritte ausführen, um die Instance auf ihre IPv6-Adresse aufmerksam zu machen. In diesem Handbuch zeigen wir Ihnen die zusätzlichen Schritte, die Sie für Nginx-Instances ausführen müssen.

Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies noch nicht geschehen ist:

- Erstellen Sie eine Nginx-Instance in Lightsail. Weitere Informationen finden Sie unter Erstellen einer Instance.
- Aktivieren Sie IPv6 für Ihre Nginx-Instance. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren von IPv6.

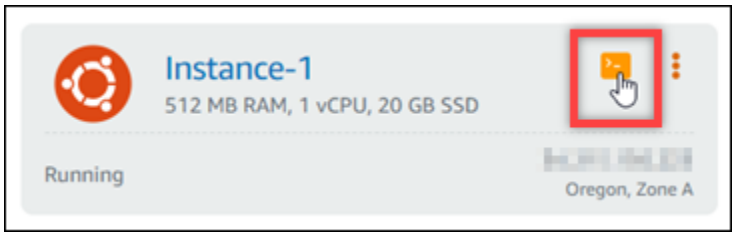
> **Note**
>
> Neue Nginx-Instance, die am oder nach dem 12. Januar 2021 erstellt wurden, sind IPv6 standardmäßig aktiviert, wenn sie in der Lightsail-Konsole erstellt werden. Sie müssen die folgenden Schritte in diesem Handbuch ausführen, um IPv6 für Ihre Instance zu konfigurieren, selbst wenn IPv6 beim Erstellen der Instance standardmäßig aktiviert war.

Konfigurieren von IPv6 auf einer Nginx-Instance

Führen Sie das folgende Verfahren aus, um IPv6 auf einer Nginx-Instance in Lightsail zu konfigurieren.

1. Melden Sie sich bei der Lightsail-Konsole an.
2.
   > **Important**
   >
   > Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um über IPv6 SSH oder RDP in Ihre Instance zu senden. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

   Suchen Sie im Abschnitt Instances der Lightsail-Startseite die Ubuntu-16-Instance, die Sie konfigurieren möchten, und wählen Sie das browserbasierte SSH-Client-Symbol aus, um eine Verbindung mit ihr über SSH herzustellen.

3. Nachdem Sie eine Verbindung zu Ihrer Instance hergestellt haben, geben Sie den folgenden Befehl ein, um zu ermitteln, ob Ihre Instance IPv6-Anforderungen über Port 80 abhört. Stellen Sie sicher, dass Sie ersetzen *<IPv6Address>* mit der Ihrer Instance zugewiesenen IPv6-Adresse.

   ```
   curl -g -6 'http://[<IPv6Address>]'
   ```

Beispiel:

```
curl -g -6 'http://[2001:0db8:85a3:0000:0000:8a2e:0370:7334]'
```

Es wird eine Antwort ähnlich dem folgenden Beispiel angezeigt:

- Wenn Ihre Instance IPv6-Anforderungen über Port 80 nicht abhört, sehen Sie eine Antwort mit einem Verbindung konnte nicht hergestellt werden Fehlermeldung. Sie sollten die Schritte 4 bis 9 dieses Verfahrens fortsetzen.

- Wenn Ihre Instance IPv6-Anforderungen über Port 80 abhört, wird eine Antwort mit dem HTML-Code der Homepage Ihrer Instanz angezeigt, wie im folgenden Beispiel gezeigt. Sie sollten hier anhalten. Sie müssen die Schritte 4 bis 9 dieses Verfahrens nicht ausführen, da Ihre Instance bereits für IPv6 konfiguriert ist.

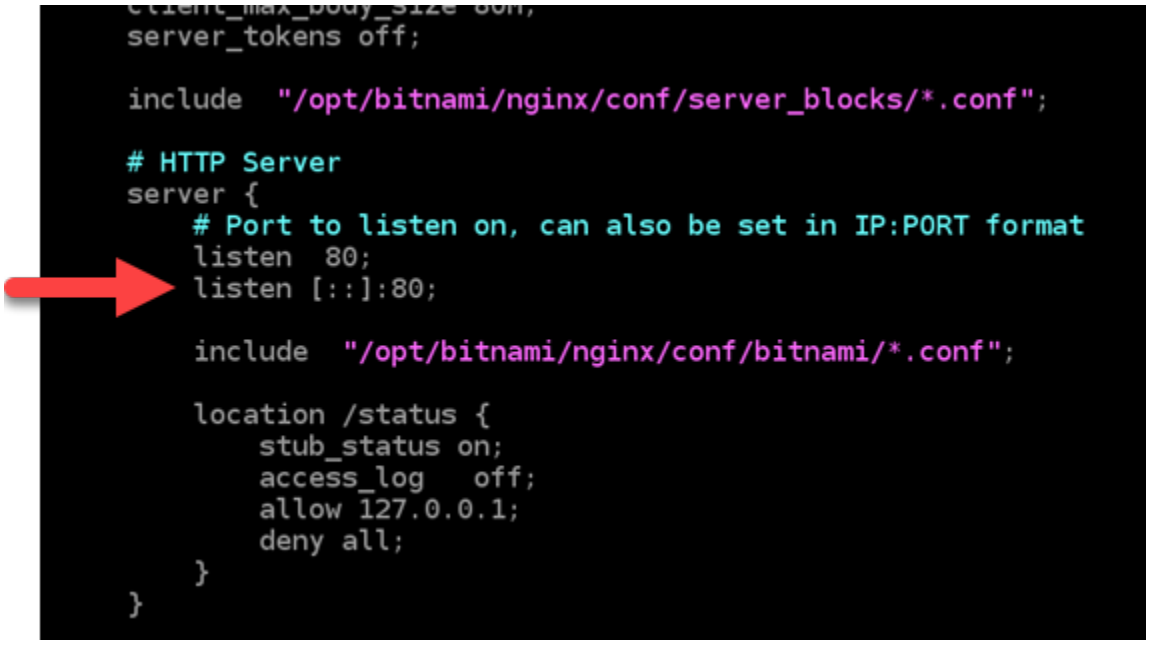
4. Geben Sie den folgenden Befehl ein, um die ngix.conf-Konfigurationsdatei mit Vim zu öffnen.

```
sudo vim /opt/bitnami/nginx/conf/nginx.conf
```

5. Drücken Sie `I`, um den Einfügemodus in Vim einzugeben.
6. Fügen Sie den folgenden Text unter dem `listen 80;`-Text, der sich bereits in der Datei befindet. Möglicherweise müssen Sie in Vim nach unten scrollen, um den Abschnitt zu sehen, in dem Sie den Text hinzufügen müssen.

```
listen [::]:80;
```

Wenn Sie fertig sind, sieht die Datei wie folgt aus:



7. Drücken Sie die Esc-Taste, um den Einfügemodus in Vim zu verlassen, geben Sie dann `:wq!` ein und drücken Sie die Enter-Taste, um Ihre Änderungen zu speichern (schreiben) und Vim zu beenden.
8. Geben Sie den folgenden Befehl ein, um die Services auf der Instance neu zu starten.

   ```
   sudo /opt/bitnami/ctlscript.sh restart
   ```
9. Geben Sie den folgenden Befehl ein, um zu ermitteln, ob Ihre Instance IPv6-Anforderungen über Port 80 abhört. Stellen Sie sicher, dass Sie *<IPv6Address>* mit der Ihrer Instance zugewiesenen IPv6-Adresse ersetzen.

   ```
   curl -g -6 'http://[<IPv6Address>]'
   ```

   Beispiel:

   ```
   curl -g -6 'http://[2001:0db8:85a3:0000:0000:8a2e:0370:7334]'
   ```

   Es wird eine Antwort ähnlich dem folgenden Beispiel angezeigt. Wenn Ihre Instanz IPv6-Anfragen über Port 80 abhört, wird eine Antwort mit dem HTML-Code der Homepage Ihrer Instance angezeigt.

Konfigurieren von IPv6 auf Plesk-Instances in Lightsail

Allen Instances in Amazon Lightsail sind standardmäßig eine öffentliche und eine private IPv4-Adresse zugewiesen. Optional können Sie IPv6 aktivieren, damit Ihren Instance eine öffentliche IPv6-Adresse zugewiesen wird. Weitere Informationen finden Sie unter Amazon Lightsail-IP-Adressen und Aktivieren oder Deaktivieren von IPv6.

Nachdem Sie IPv6 für eine Instances aktiviert haben, die den Plesk-Blueprint verwendet, müssen Sie weitere Schritte ausführen, um die Instance auf ihre IPv6-Adresse aufmerksam zu machen. In diesem Handbuch zeigen wir Ihnen die zusätzlichen Schritte, die Sie für Plesk-Instances ausführen müssen.

Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies noch nicht geschehen ist:

- Erstellen einer &lightsail;-Instance, die Plesk ausführt Weitere Informationen finden Sie unter Erstellen einer Instance.
- Aktivieren Sie IPv6 für Ihre Plesk-Instance. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren von IPv6.

> **Note**
>
> Neue Plesk-Instances, die am oder nach dem 12. Januar 2021 erstellt wurden, sind IPv6 standardmäßig aktiviert, wenn sie in der Lightsail-Konsole erstellt werden. Sie müssen die folgenden Schritte in diesem Handbuch ausführen, um IPv6 für Ihre Instance zu konfigurieren, selbst wenn IPv6 beim Erstellen der Instance standardmäßig aktiviert war.

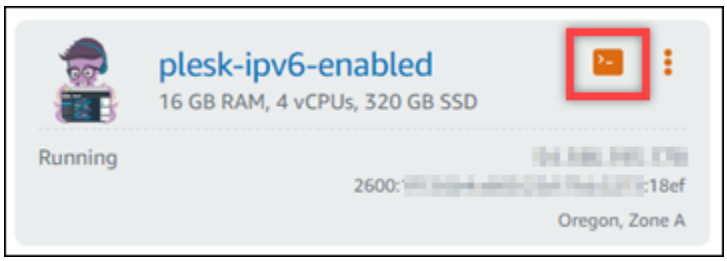
Konfigurieren von IPv6 auf einer Plesk-Instance

Führen Sie das folgende Verfahren aus, um IPv6 für eine Plesk-Instance in Lightsail zu konfigurieren.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. **Important**

   Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um SSH oder RDP über IPv6 in Ihre Instance zu übertragen. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

   Suchen Sie im Abschnitt Instances der Lightsail-Startseite die Plesk-Instance, die Sie konfigurieren möchten, und wählen Sie das browserbasierte SSH-Client-Symbol aus, um über SSH eine Verbindung zu ihr herzustellen.

3. Nachdem Sie eine Verbindung mit der Instance hergestellt haben, geben Sie den folgenden Befehl ein, um die für Ihre Instance konfigurierten IP-Adressen anzuzeigen.

   ```
   ip addr
   ```

   Es wird eine Antwort ähnlich dem folgenden Beispiel angezeigt:

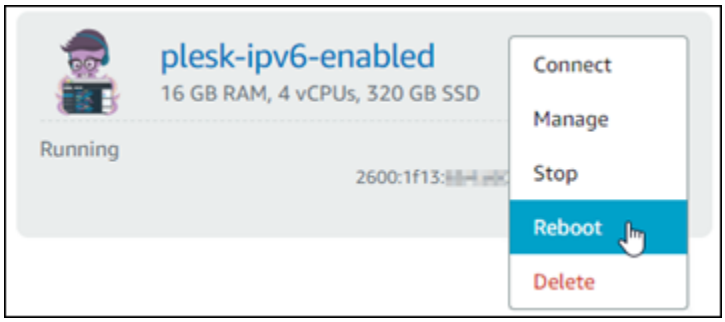
   - Wenn Ihre Instance ihre IPv6-Adresse nicht erkennt, wird sie in der Antwort nicht aufgeführt. Sie sollten die Schritte 4 bis 7 dieses Verfahrens fortsetzen.

```
admin@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80:[redacted]:3df7/64 scope link
       valid_lft forever preferred_lft forever
```

- Wenn Ihre Instance ihre IPv6-Adresse erkennt, wird sie in der Antwort mit einem `scope global`, wie in diesem Beispiel gezeigt. Sie sollten hier anhalten. Sie müssen die Schritte 4 bis 7 dieses Verfahrens nicht ausführen, da Ihre Instance bereits so konfiguriert ist, dass sie ihre IPv6-Adresse erkennt.

```
admin@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2600:1f13:[redacted]:f383:3212/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80:[redacted]:3df7/64 scope link
       valid_lft forever preferred_lft forever
```

4. Wechseln Sie zurück zur Lightsail-Konsole.
5. In der Instances wählen Sie auf der Registerkarte „Lightsail -Startseite das Aktionsmenü () für die Plesk-Instance aus und wählen SieNeustartaus.



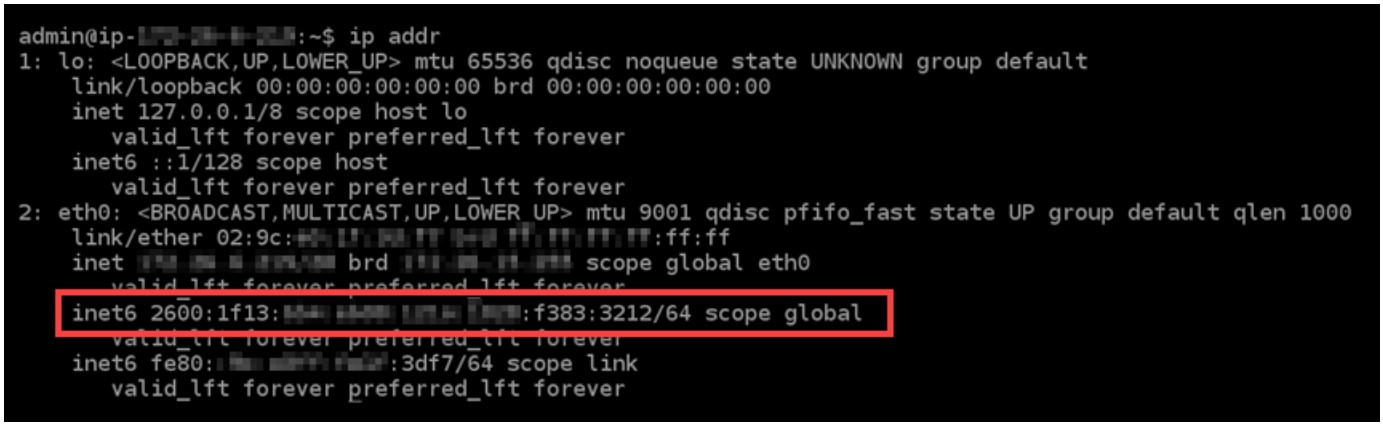
Warten Sie einige Minuten, bis Ihre Instance neu gestartet wird, bevor Sie mit dem nächsten Schritt fortfahren.

6. Wechseln Sie zurück zur SSH-Sitzung Ihrer Plesk-Instance.

7. Geben Sie den folgenden Befehl ein, um die für Ihre Instance konfigurierten IP-Adressen anzuzeigen, und bestätigen Sie, dass die zugewiesene IPv6-Adresse jetzt erkannt wird.

```
ip addr
```

Es wird eine Antwort ähnlich dem folgenden Beispiel angezeigt. Wenn Ihre Instance ihre IPv6-Adresse erkennt, wird sie in der Antwort mit der Bezeichnung `scope global`, wie in diesem Beispiel gezeigt.



Konfigurieren von IPv6 für Ubuntu-16-Instances in Lightsail

Allen Instances in Amazon Lightsail sind standardmäßig eine öffentliche und eine private IPv4-Adresse zugewiesen. Optional können Sie IPv6 aktivieren, damit Ihren Instance eine öffentliche IPv6-Adresse zugewiesen wird. Weitere Informationen finden Sie unter IP-Adressen und Aktivieren oder Deaktivieren von IPv6 in Amazon Lightsail.

Nachdem Sie IPv6 für eine Instance aktiviert haben, die den Ubuntu-16-Blueprint verwendet, müssen Sie weitere Schritte ausführen, um die Instance auf ihre IPv6-Adresse aufmerksam zu machen. In diesem Handbuch zeigen wir Ihnen die zusätzlichen Schritte, die Sie für Ubuntu-16-Instances ausführen müssen.

Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies noch nicht geschehen ist:

- Erstellen Sie eine Ubuntu-16-Instance in Lightsail. Weitere Informationen finden Sie unter Erstellen einer Instance.

- Aktivieren Sie IPv6 für Ihre Ubuntu-16-Instance. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren von IPv6.

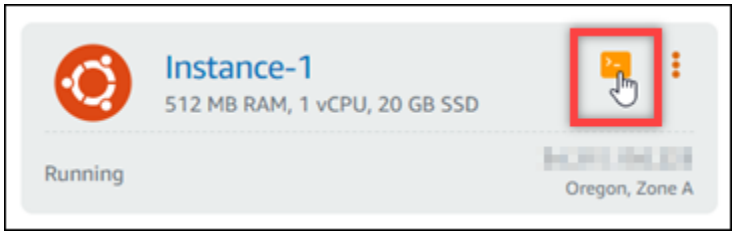
> **Note**
>
> Neue Ubuntu-Instances, die am oder nach dem 12. Januar 2021 erstellt wurden, sind IPv6 standardmäßig aktiviert, wenn sie in der Lightsail -Konsole erstellt werden. Sie müssen die folgenden Schritte in diesem Handbuch ausführen, um IPv6 für Ihre Instance zu konfigurieren, selbst wenn IPv6 beim Erstellen der Instance standardmäßig aktiviert war.

So konfigurieren Sie eine laufende Ubuntu Server 16-Instance

Führen Sie das folgende Verfahren aus, um IPv6 auf einer Ubuntu-16-Instance in Lightsail zu konfigurieren.

1. Melden Sie sich bei der Lightsail-Konsole an.
2.
> **Important**
>
> Die browserbasierten Lightsail-SSH/RDP-Clients akzeptieren nur IPv4-Datenverkehr. Verwenden Sie einen Drittanbieter-Client, um SSH oder RDP über IPv6 in Ihre Instance zu übertragen. Weitere Informationen finden Sie unter Eine Verbindung mit Ihren Instances herstellen.

   Suchen Sie im Abschnitt Instances der Lightsail-Startseite die Ubuntu-16-Instance, die Sie konfigurieren möchten, und wählen Sie das browserbasierte SSH-Client-Symbol aus, um eine Verbindung mit ihr über SSH herzustellen.

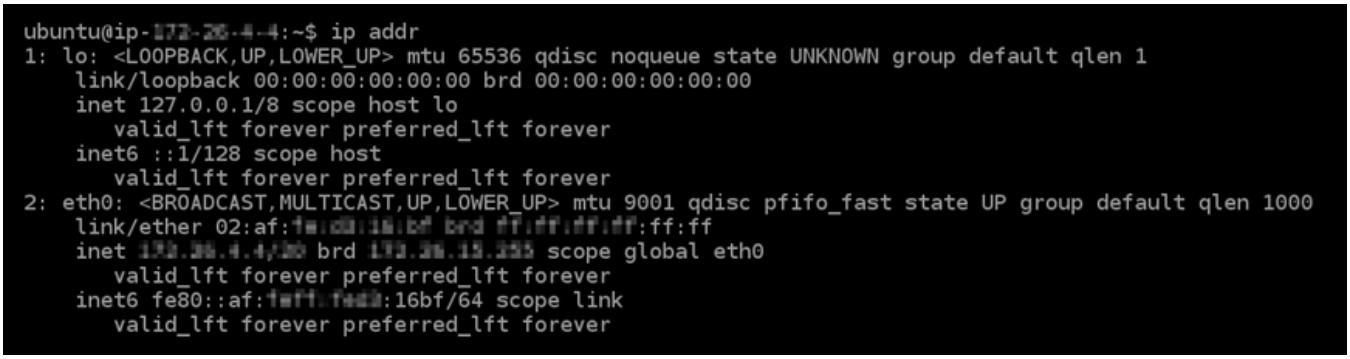


3. Nachdem Sie eine Verbindung mit der Instance hergestellt haben, geben Sie den folgenden Befehl ein, um die für Ihre Instance konfigurierten IP-Adressen anzuzeigen.

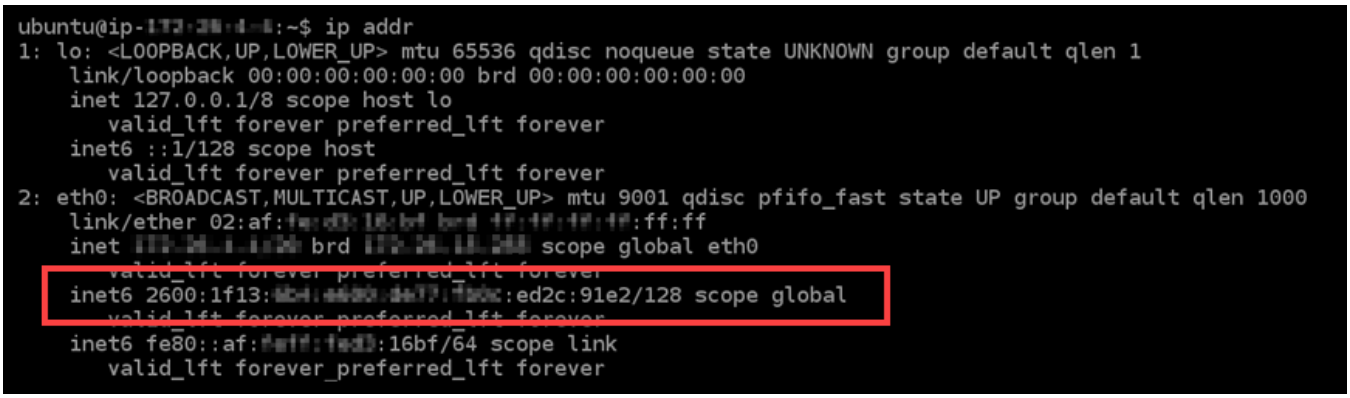
```
ip addr
```

Es wird eine Antwort ähnlich dem folgenden Beispiel angezeigt:

- Wenn Ihre Instance ihre IPv6-Adresse nicht erkennt, wird sie in der Antwort nicht aufgeführt. Sie sollten die Schritte 4 bis 9 dieses Verfahrens fortsetzen.



- Wenn Ihre Instance ihre IPv6-Adresse erkennt, wird sie in der Antwort mit einem `scope global`, wie in diesem Beispiel gezeigt. Sie sollten hier anhalten. Sie müssen die Schritte 4 bis 9 dieses Verfahrens nicht ausführen, da Ihre Instance bereits so konfiguriert ist, dass sie ihre IPv6-Adresse erkennt.



4. Geben Sie den folgenden Befehl ein, um die Schnittstellen-Konfigurationsdatei mit Vimzu öffnen.

```
sudo vim /etc/network/interfaces
```

5. Drücken Sie I, um den Einfügemodus in Vim einzugeben.
6. Fügen Sie die folgende Zeile am Ende der Datei hinzu.

```
iface eth0 inet6 dhcp
```

Wenn Sie fertig sind, sieht die Datei wie folgt aus:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# Source interfaces
# Please check /etc/network/interfaces.d before changing this file
# as interfaces may have been defined in /etc/network/interfaces.d
# See LP: #1262951
source /etc/network/interfaces.d/*.cfg

iface eth0 inet6 dhcp
```

7. Drücken Sie die Esc-Taste, um den Einfügemodus in Vim zu verlassen, geben Sie dann `:wq!` ein und drücken Sie die Enter-Taste, um Ihre Änderungen zu speichern (schreiben) und Vim zu beenden.
8. Geben Sie den folgenden Befehl ein, um die Services auf der Instance neu zu starten.

   ```
   sudo service networking restart
   ```

   Möglicherweise müssen Sie noch einige Minuten warten, damit Ihre Instance ihre IPv6-Adresse erkennt, nachdem Sie den Netzwerkdienst Ihrer Instance neu gestartet haben.
9. Geben Sie den folgenden Befehl ein, um die für Ihre Instance konfigurierten IP-Adressen anzuzeigen, und bestätigen Sie, dass die zugewiesene IPv6-Adresse jetzt erkannt wird.

   ```
   ip addr
   ```

   Es wird eine Antwort ähnlich dem folgenden Beispiel angezeigt. Wenn Ihre Instance ihre IPv6-Adresse erkennt, wird sie in der Antwort mit der Bezeichnung `scope global`, wie in diesem Beispiel gezeigt.

```
ubuntu@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:af:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2600:1f13:[redacted]:ed2c:91e2/128 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::af:[redacted]:16bf/64 scope link
       valid_lft forever preferred_lft forever
```

Arbeiten mit Amazon Lightsail

In den folgenden Anleitungen erfahren Sie mehr über verschiedene Aufgaben, die Sie in Lightsail fertigstellen können. Sie können beispielsweise eine HAR-Datei zur Fehlerbehebung erstellen, eine LAMP-Instance starten und konfigurieren oder Ihre MySQL-Datenbank migrieren.

Themen

Arbeiten mit AWS Command Line Interface in Lightsail

Die AWS Command Line Interface (AWS CLI) ist ein Tool, mit dem fortgeschrittene Benutzer und Entwickler den Amazon Lightsail-Service steuern können, indem Befehle im Terminal (unter Linux und Unix) oder in der Eingabeaufforderung (unter Windows) eingegeben werden. Sie können Lightsail auch über die Lightsail-Konsole, eine grafische Benutzeroberfläche und die Lightsail Anwendungsprogrammschnittstelle (API) steuern.

In Lightsail können Sie die AWS CLI auf Ihrem lokalen Desktop oder auf Ihrer Lightsail-Instance installieren.

Weitere Informationen zur AWS CLI finden Sie im Benutzerhandbuch zu AWS Command Line Interface. Die Amazon Lightsail-Befehle finden Sie in der AWS CLI-Befehlsreferenz.

- Informationen zum Installieren der AWS CLI auf Ihrem lokalen Desktop finden Sie unter Installieren der AWS CLI in der AWS Command Line Interface-Dokumentation.
- Zur Installation der AWS CLI auf Ihrer Ubuntu-basierten Lightsail-Instance stellen Sie eine Verbindung mit Ihrer Instance her und geben dann `sudo apt-get -y install awscli` ein.

> **Note**
>
> Die AWS CLI sollte bereits auf der Amazon Linux Lightsail-Instance installiert sein. Wenn Sie sie erneut installieren müssen, stellen Sie eine Verbindung zu Ihrer Instance her und geben Sie `sudo yum install aws-cli` ein.

Nachdem Sie die AWS CLI installiert haben, müssen Sie Zugriffsschlüssel abrufen und dann die AWS CLI konfigurieren, um sie verwenden zu können. Weitere Informationen finden Sie unter Erstellen eines Zugriffsschlüssels zur Verwendung der Lightsail-API oder der AWS Command Line Interface.

Erstellen eines Zugriffsschlüssels für die Verwendung der Lightsail-API oder der AWS Command Line Interface.

Für die Verwendung der Lightsail-API oder der AWS Command Line Interface (AWS CLI) müssen Sie einen neuen Zugriffsschlüssel erstellen. Jeder Zugriffschlüssel besteht aus einer Access Key ID (Zugriffsschlüssel-ID) und einem Secret Access Key (geheimen Schlüssel). Verwenden Sie die folgenden Verfahren zum Erstellen des Schlüssels und zum Konfigurieren der AWS CLI, um die Lightsail-API aufrufen zu können.

Schritt 1: Erstellen Sie einen neuen Zugriffsschlüssel

Sie können auf der AWS Identity and Access Management (IAM)-Konsole einen neuen Zugriffsschlüssel erstellen.

1. Melden Sie sich bei der IAM-Konsole an.

2. Wählen Sie den Namen des Benutzers, für den Sie einen Zugriffsschlüssel erstellen möchten. Der Benutzer, den Sie auswählen, sollte vollen Zugriff oder bestimmten Zugriff auf Lightsail-Aktionen.
3. Wechseln Sie zur Registerkarte Security credentials (Sicherheitsanmeldeinformationen).
4. Klicken Sie auf Erstellen eines Zugriffsschlüssels unter dem Verzeichnis Zugriffsschlüssel-Abschnitt der Seite.

   > **Note**
   >
   > Sie können maximal zwei Zugriffsschlüssel ("aktiv" oder "inaktiv") gleichzeitig haben. Wenn Sie bereits zwei Zugriffschlüssel besitzen, müssen Sie ein Schlüsselpaar löschen, bevor Sie ein neues erstellen. Stellen Sie sicher, dass ein Zugriffsschlüssel nicht aktiv verwendet wird, bevor Sie ihn löschen.

5. Merken Sie sich die folgenden Informationen Zugriffsschlüssel-ID und Geheimer Zugriffsschlüssel-Liste. Klicken Sie auf Anzeigen unter dem Verzeichnis Geheimer Zugriffsschlüssel, um Ihre Geheimen Zugriffsschlüssel zu sehen.

   Sie können sie von diesem Bildschirm kopieren oder Download Key File (Schlüsseldatei herunterladen) wählen, um eine .csv-Datei mit den Zugriffsschlüsseln herunterzuladen.

   > **Important**
   >
   > Bewahren Sie Ihre Zugriffsschlüssel an einem sicheren Ort auf. Sie sollten der Datei einen Namen wie beispielweise `MyLightsailKeys.csv` geben, sodass Sie sie später leicht wiederfinden. Wenn Sie die CSV-Datei von der IAM-Konsole heruntergeladen haben, sollten Sie sie löschen, nachdem Sie Schritt 2 abgeschlossen haben. Sie können später neue Zugriffsschlüssel erstellen.

Schritt 2: Konfigurieren der AWS CLI

Wenn Sie die AWS CLI nicht installiert habe, können Sie das jetzt machen. Siehe Installieren der AWS Command Line Interface. Nach der Installation der AWS CLI müssen Sie diese konfigurieren, sodass Sie sie verwenden können.

1. Öffnen Sie ein Terminal-Fenster oder eine Eingabeaufforderung.
2. Typ `aws configure`.

3. Fügen Sie Ihre AWS-Zugriffsschlüssel-ID aus der .csv-Datei ein, die Sie im vorherigen Schritt erstellt haben.
4. Fügen Sie Ihren geheimen AWS-Zugriffsschlüssel ein, wenn Sie dazu aufgefordert werden.
5. Geben Sie die AWS-Region ein, in der sich Ihre Ressourcen befinden. Wenn sich Ihre Ressourcen beispielsweise hauptsächlich in Ohio befinden, wählen Sie `us-east-2`, wenn Sie nach dem Default region name (Standard-Regionsnamen) gefragt werden.

   Weitere Informationen zur Verwendung der AWS CLI-Option `--region` finden Sie unter Allgemeine Optionen in der AWS CLI-Referenz.
6. Wählen Sie ein Default output format (Standard-Ausgabeformat), z. B. `json`.

Nächste Schritte

- Installieren des SDK
- Konfigurieren der AWS Command Line Interface für die Arbeit mit Amazon Lightsail
- Lesen Sie die API-Dokumentationen

AWS CloudShell in Lightsail

AWS CloudShell ist eine browserbasierte, vorauthentifizierte Shell, die Sie direkt über die Amazon Lightsail-Konsole starten können. Verwenden Sie CloudShell , um Ihre Lightsail-Ressourcen über die Befehlszeilenschnittstelle zu verwalten. Sie können AWS Command Line Interface (AWS CLI)-Befehle mit Ihrer bevorzugten Shell ausführen, z. B. Bash PowerShelloder Z-Shell. Sie können dies tun, ohne Befehlszeilentools herunterladen oder installieren zu müssen. Wenn Sie starten CloudShell, wird eine Datenverarbeitungsumgebung erstellt, die auf Amazon Linux 2 basiert. In dieser Umgebung können Sie auf eine Vielzahl vorinstallierter Entwicklungstools zugreifen, wie z. B. die AWS CLI. Eine vollständige Liste der vorinstallierten Tools finden Sie unter Vorinstallierte Software im CloudShell - Benutzerhandbuch.

Persistenter Speicher

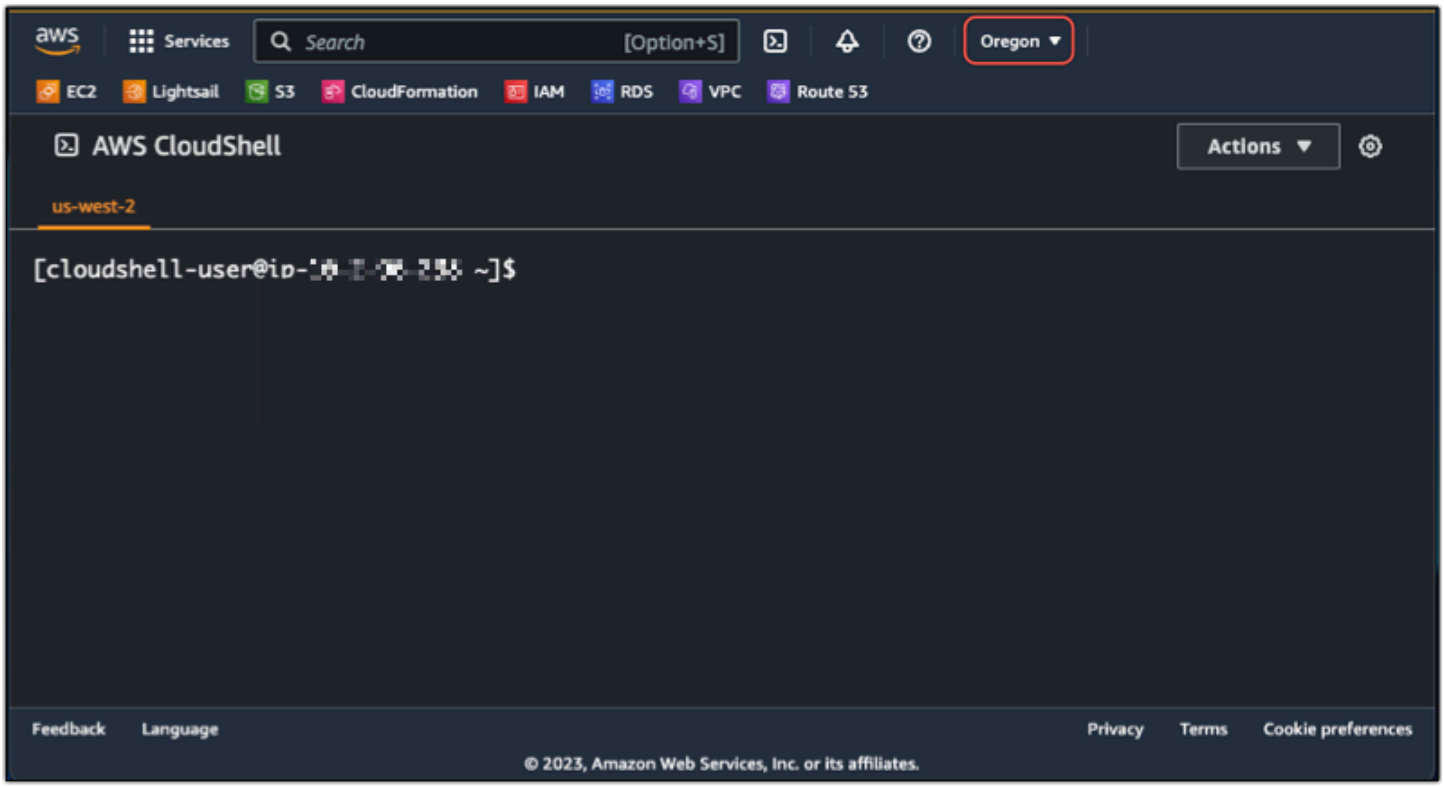
Mit können AWS CloudShell Sie bis zu 1 GB persistenten Speicher pro AWS-Region ohne zusätzliche Kosten verwenden. Der persistente Speicher befindet sich in Ihrem Home-Verzeichnis (`$HOME`) und ist für Sie privat. Im Gegensatz zu kurzlebigen Umgebungsressourcen, die nach dem Ende jeder Shell-Sitzung gelöscht werden, bleiben Daten in Ihrem Home-Verzeichnis zwischen den

Sitzungen bestehen. Weitere Informationen zur Aufbewahrung von Daten im persistenten Speicher finden Sie unter Persistenter Speicher im CloudShell -Benutzerhandbuch.

AWS-Regionen

In Lightsail wird eine CloudShell Sitzung in der geöffnet AWS-Region , die die geringste Latenz zu Ihrem physischen Standort bietet. Das bedeutet, dass zwischen den Sitzungen wechseln AWS-Regionen kann. Notieren Sie sich, in welcher AWS-Region sich Ihre CloudShell Sitzung befindet, damit Sie den persistenten Speicher von 1 GB verwenden können. Um die AWS-Region der Sitzung zu ändern, wählen Sie das Symbol In neuer Browser-Registerkarte öffnen. Dies bietet die Möglichkeit, in einem neuen Browserfenster auf Ihre CloudShell Sitzung zuzugreifen.

Wählen Sie auf der Navigationsleiste der neuen Browser-Registerkarte den Namen der AWS-Region aus, der aktuell angezeigt wird. Wählen Sie dann die aus AWS-Region , zu der Sie wechseln möchten.



Weitere Informationen zu CloudShellfinden Sie im CloudShell -Benutzerhandbuch.

Starten und verwenden AWS CloudShell

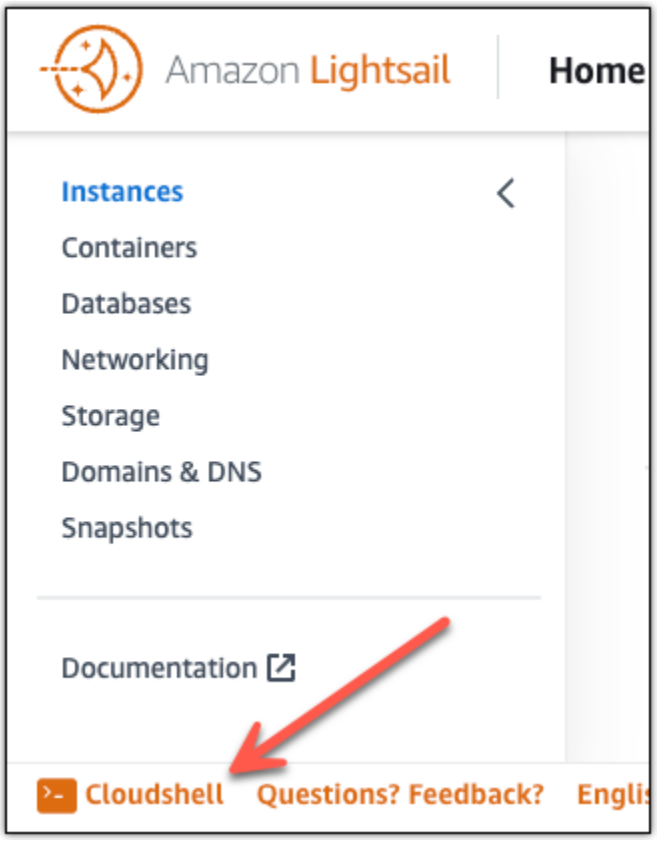
Erfahren Sie, wie Sie eine - AWS CloudShell Sitzung in Lightsail starten und verwenden. Wenn Sie nicht über die Berechtigung zum Ausführen von verfügen CloudShell, müssen Sie die `arn:aws:iam::aws:policy/AWSCloudShellFullAccess` Richtlinie der AWS Identity and Access Management (IAM)-Identität hinzufügen, die Sie verwenden. Wenn Sie die `arn:aws:iam::aws:policy/AdministratorAccess` Richtlinie bereits angehängt haben, sollten Sie auf zugreifen können CloudShell. Weitere Informationen finden Sie unter ???.

Starten AWS CloudShell

Sie können CloudShell über die Amazon Lightsail-Konsole starten. Nach Beginn der Sitzung können Sie zu Ihrer bevorzugten Shell wechseln, z. B. `Bash`, `PowerShell` oder`Z shell`.

Führen Sie die folgenden Schritte aus, um eine neue AWS CloudShell Sitzung in Lightsail zu starten:

1. Melden Sie sich bei der Lightsail-Konsole unter https://lightsail.aws.amazon.com/ an.
2. Wählen Sie CloudShell in der Konsolen-Symbolleiste unten links in der Konsole aus. Wenn die Eingabeaufforderung angezeigt wird, ist die Shell für die Interaktion bereit.



3. (Optional) Um eine vorinstallierte Shell auszuwählen, mit der Sie arbeiten möchten, geben Sie an der Befehlszeile einen der folgenden Programmnamen ein:

   Bash: **`bash`**

   Wenn Sie zu Bash wechseln, wird das Symbol in der Befehlszeile auf $ aktualisiert. Bash ist die Standard-Shell in AWS CloudShell.

   PowerShell: **`pwsh`**

   Wenn Sie zu wechseln PowerShell, wird das Symbol in der Eingabeaufforderung auf aktualisiertPS>.

   Z shell: **`zsh`**

   Wenn Sie zu Z shell wechseln, wird das Symbol in der Befehlszeile auf % aktualisiert.

Example Beispiel für einen Lightsail-API-Befehl in AWS CloudShell

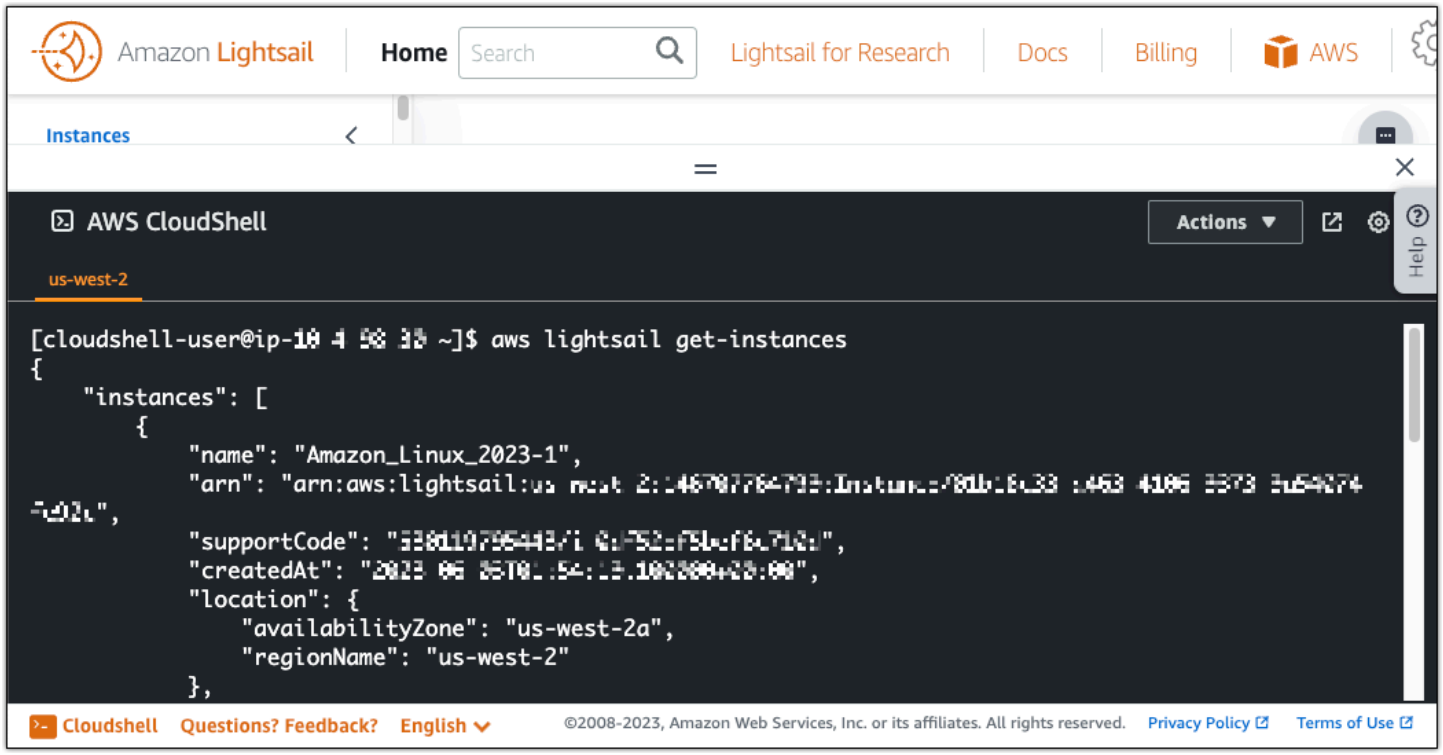
Es gibt mehrere Befehlszeilen-Tools, die in der CloudShell Sitzung vorinstalliert sind und die Sie verwenden können. In diesem Beispiel verwenden Sie die Lightsail`GetInstances`-API-Operation,

um die Instances anzuzeigen, die sich in Ihrem Lightsail-Konto befinden. Weitere Informationen zur `GetInstances`-API-Operation finden Sie unter GetInstances in der Amazon Lightsail-API-Referenz.

1. Melden Sie sich bei der Lightsail-Konsole unter https://lightsail.aws.amazon.com/ an.
2. Wählen Sie CloudShell in der Konsolen-Symbolleiste unten links in der Konsole aus.
3. Geben Sie nach der AWS CloudShell Eingabeaufforderung den folgenden Befehl ein:

   ```
   aws lightsail get-instances
   ```

   Sie sollten jetzt eine vollständige Liste der Instances sehen, die sich in Ihrem Lightsail-Konto befinden.



Zusätzliche Informationen

Weitere Informationen zu finden Sie in der folgenden Dokumentation AWS CloudShell:

- Amazon Lightsail-API-Referenz
- Häufig gestellte Fragen in AWS CloudShell
- Unterstützte Browser in AWS CloudShell

- Fehlerbehebung in AWS CloudShell
- Arbeiten mit AWS-Services in AWS CloudShell

Protokollierung von Lightsail-API-Aufrufen mit AWS CloudTrail

Amazon Lightsail ist in AWS CloudTrail integriert, einen Service, der die Aktionen eines Benutzers, einer Rolle oder eines AWS-Service in Lightsail protokolliert. CloudTrail erfasst alle API-Aufrufe für Lightsail als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Lightsail-Konsole und Code-Aufrufe der Lightsail-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon S3-Bucket, einschließlich Ereignisse für Lightsail aktivieren. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Event history (Ereignisverlauf) anzeigen. Mit den von CloudTrail erfassten Informationen können Sie die an Lightsail gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail-Benutzerhandbuch.

Lightsail-Informationen in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Kontos für Sie aktiviert. Die in Lightsail auftretenden Aktivitäten werden als CloudTrail-Ereignis zusammen mit anderen AWS-Serviceereignissen in Event History (Ereignisverlauf). aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf.

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für Lightsail, erstellen Sie einen Trail. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Wenn Sie einen Pfad in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- Von CloudTrail unterstützte Dienste und Integrationen
- Konfigurieren von Amazon-SNS-Benachrichtigungen für CloudTrail

- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien aus mehreren Konten

Alle Lightsail-Aktionen werden von CloudTrail protokolliert und sind in der Amazon Lightsail-API-Referenz dokumentiert. Zum Beispiel werden Einträge in den CloudTrail-Protokolldateien generiert, wenn Aufrufe an die Abschnitte GetInstance, AttachStaticIp und RebootInstance erfolgen.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter dem CloudTrail userIdentity-Element.

Grundlagen von Lightsail-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Tutorial: Verbinden einer Lightsail-LAMP-Instance mit einer Aurora-Datenbank

Anwendungsdaten für Beiträge, Seiten und Benutzer werden in einer MariaDB-Datenbank gespeichert, die auf der LAMP-Instance in Amazon Lightsail ausgeführt wird. Wenn die WordPress-Instance ausfällt, können Sie Ihre Daten möglicherweise nicht wiederherstellten. Um dieses Szenario zu vermeiden, sollten Sie Ihre Anwendungsdaten in eine von MySQL verwaltete Datenbank übertragen.

Amazon Aurora ist eine mit MySQL und PostgreSQL kompatible relationale Datenbank, die für die Cloud entwickelt wurde. Sie kombiniert die Leistung und Verfügbarkeit traditioneller Unternehmensdatenbanken mit der Einfachheit und Kosteneffizienz von Open-Source-Datenbanken. Aurora ist Teil von Amazon Relational Database Service (Amazon RDS). Amazon RDS ist ein verwalteter Datenbakservice, der das Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der Cloud vereinfacht. Weitere Informationen finden Sie im Benutzerhandbuch für Amazon Relational Database Service und im Benutzerhandbuch für Amazon Aurora.

In diesem Tutorial zeigen wir Ihnen, wie Sie Ihre Anwendungsdatenbank von einer LAMP-Instance in Lightsail mit einer von Aurora verwalteten Datenbank in Amazon RDS verbinden.

Inhalt

Schritt 1: Erfüllen der Voraussetzungen

Stellen Sie vor Beginn sicher, dass die folgenden Voraussetzungen erfüllt sind:

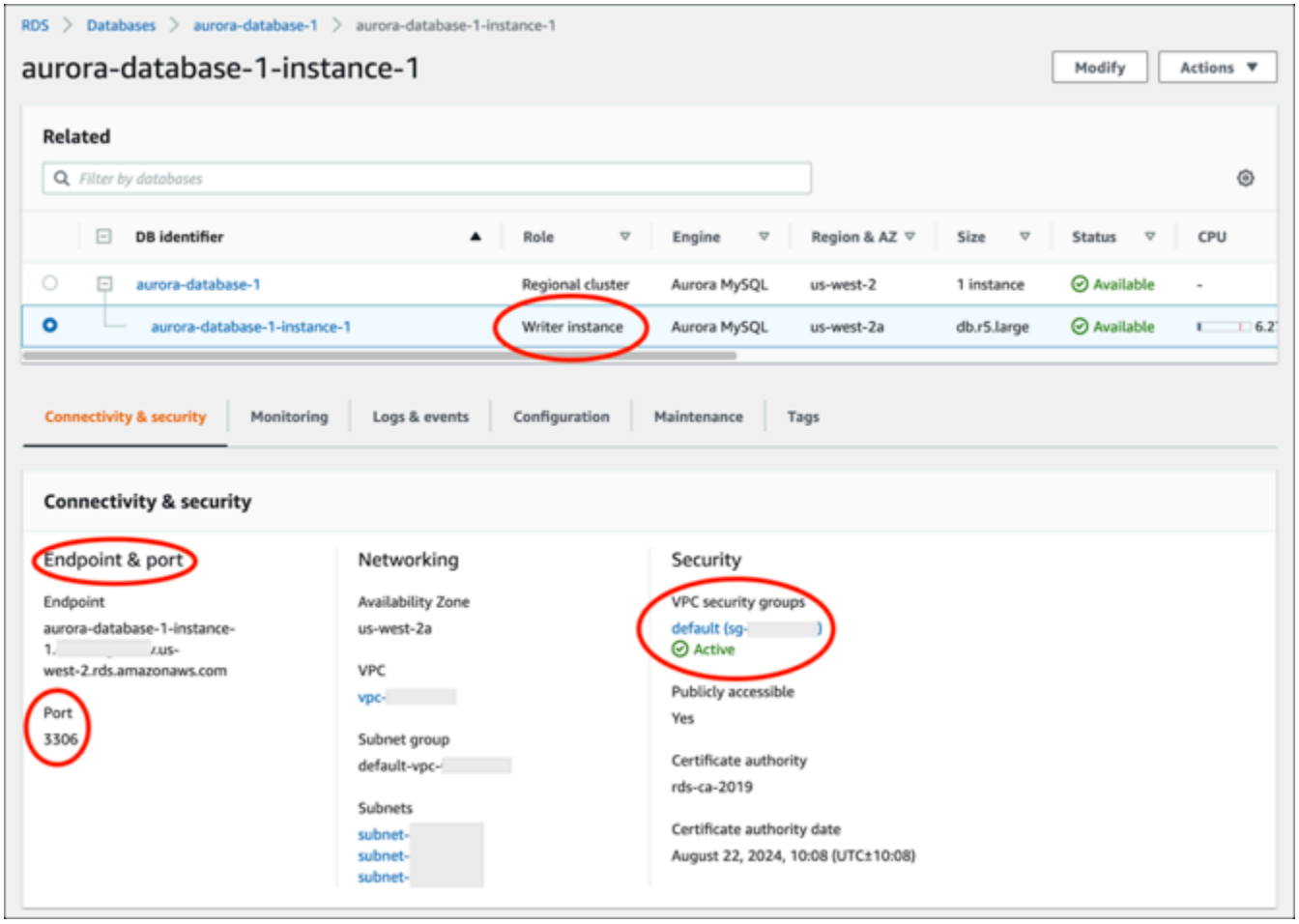
1. Erstellen Sie eine LAMP-Instance in Lightsail und konfigurieren Sie Ihre Anwendung darauf. Die Instance muss sich im laufenden Zustand befinden, bevor Sie fortfahren. Weitere Informationen finden Sie im Tutorial: Starten und Konfigurieren einer LAMP-Instance in Lightsail.
2. Aktivieren Sie in Ihrem Lightsail-Konto das VPC-Peering. Weitere Informationen finden Sie unter Einrichten von Amazon-VPC-Peering für die Zusammenarbeit mit AWS-Ressourcen außerhalb von Lightsail.
3. Erstellen einer von Aurora verwalteten Datenbank in Amazon RDS. Die Datenbank muss sich in derselben AWS-Region wie Ihre LAMP-Instance befinden. Sie muss sich auch im laufenden Zustand befinden, bevor Sie fortfahren. Weitere Informationen finden Sie unter Erste Schritte mit Amazon Aurora im Amazon-Aurora-Benutzerhandbuch.

Schritt 2: Konfigurieren der Sicherheitsgruppe für Ihre Aurora-Datenbank

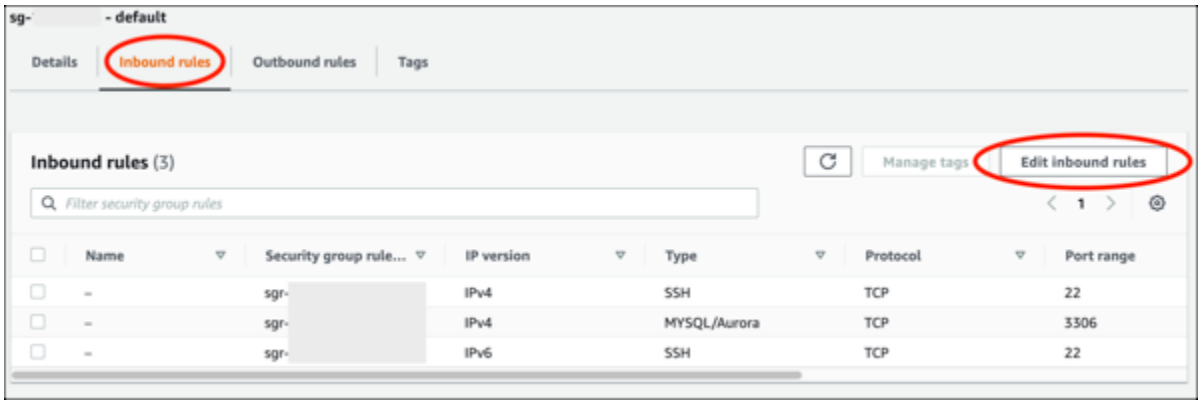
Eine AWS-Sicherheitsgruppe fungiert als virtuelle Firewall für Ihre AWS-Ressourcen. Sie kontrolliert den ein- und ausgehenden Datenverkehr, der sich mit Ihrer Aurora-Datenbank in Amazon RDS verbinden kann. Weitere Informationen finden Sie unter Kontrollieren des Datenverkehrs zu Ressourcen mithilfe von Sicherheitsgruppen im Benutzerhandbuch von Amazon Virtual Private Cloud.

Führen Sie das folgende Verfahren aus, um die Sicherheitsgruppe so zu konfigurieren, dass Ihre LAMP-Instance eine Verbindung zu Ihrer Aurora-Datenbank herstellen kann.

1. Melden Sie sich bei der Amazon-RDS-Konsole an.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie das Symbol der Writer-Instance der Aurora-Datenbank aus, mit der Ihre LAMP-Instance eine Verbindung herstellen wird.
4. Wählen Sie die Registerkarte Connectivity & security (Konnektivität und Sicherheit).
5. Notieren Sie sich aus dem Abschnitt Endpoint & Port (Endpunkt und Port) den Endpoint name (Endpunktnamen) und den Port (Port) der Writer-Instance. Sie benötigen diese Angaben später bei der Konfiguration Ihrer Lightsail-Instance zur Verbindungsherstellung mit der Datenbank.
6. Wählen Sie im Bereich Security (Sicherheit) den Link der aktiven VPC-Sicherheitsgruppe aus. Sie werden zur Sicherheitsgruppe Ihrer Datenbank weitergeleitet.



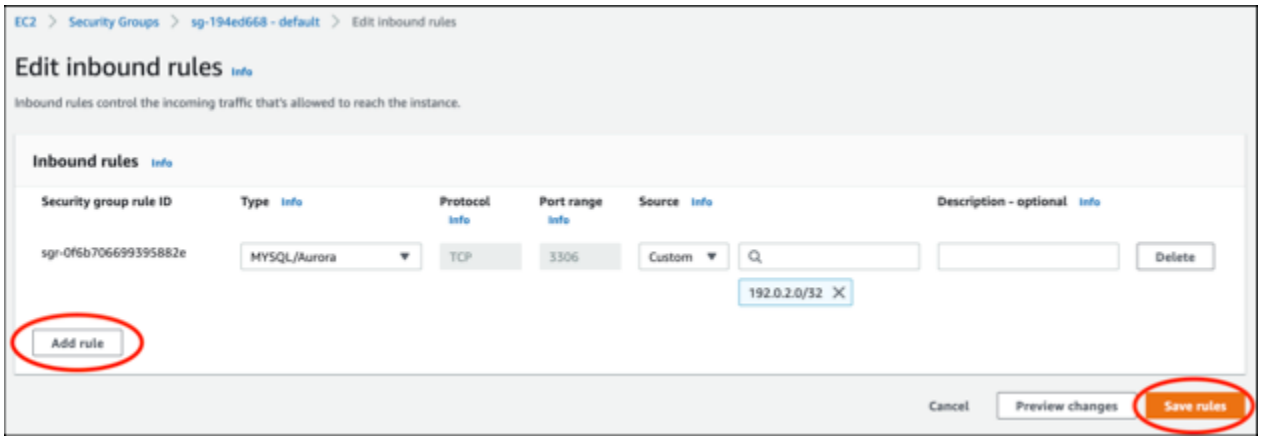
7. Vergewissern Sie sich, dass die Sicherheitsgruppe für Ihre Aurora-Datenbank ausgewählt ist.
8. Wählen Sie die Registerkarte Inbound rules (Regeln für eingehenden Datenverkehr) aus.
9. Wählen Sie Edit inbound rules (Regeln für eingehenden Datenverkehr bearbeiten) aus.



10. Wählen Sie auf der Seite Edit inbound rules (Regeln für eingehenden Datenverkehr bearbeiten) die Option Add Rule (Regel hinzufügen).
11. Führen Sie die folgenden Schritte aus:

- Wenn Sie den standardmäßigen MySQL-Port 3306 verwenden, wählen Sie MySQL/Aurora im Dropdownmenü Type (Typ) aus.
- Wenn Sie einen benutzerdefinierten Port für Ihre Datenbank verwenden, wählen Sie Custom TCP(Benutzerdefiniertes TCP) im Dropdownmenü Type (Typ) aus und geben Sie im Textfeld Port Range (Port-Bereich) die Portnummer ein.

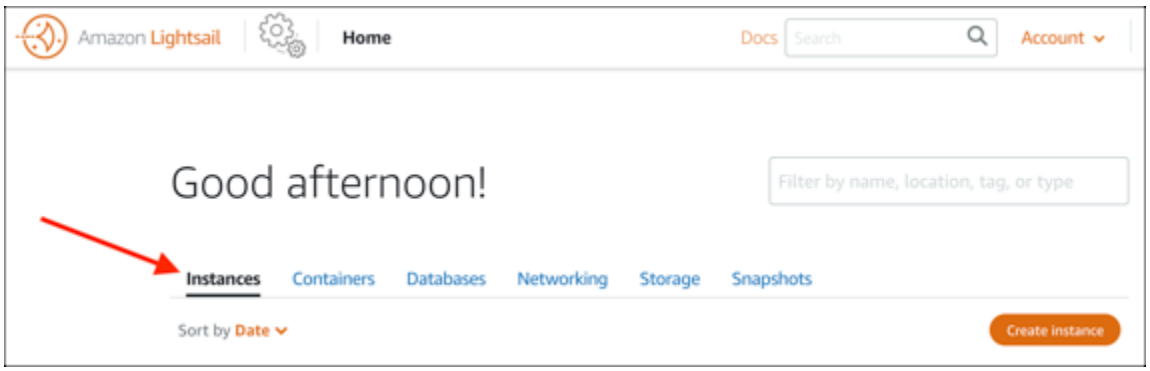
12. Fügen Sie im Textfeld Source (Quelle) die private IP-Adresse Ihrer LAMP-Instance hinzu. Sie müssen die IP-Adressen in CIDR-Notation eingeben, was bedeutet, dass Sie `/32` anhängen müssen. Zum Beispiel, um `192.0.2.0` zuzulassen, geben Sie `192.0.2.0/32` ein.
13. Wählen Sie Save rules (Regeln speichern) aus.



Schritt 3: Herstellen einer Verbindung mit Ihrer Aurora-Datenbank von Ihrer Lightsail-Instance

Schliessen Sie den folgenden Vorgang ab, um zu bestätigen, dass Sie eine Verbindung mit Ihrer Aurora-Datenbank von Ihrer Lightsail-Instance herstellen können.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Instances.



3. Wählen Sie das browserbasierte SSH-Client-Symbol für Ihre LAMP-Instance aus, um mit SSH eine Verbindung herzustellen.

4. Nachdem Sie mit Ihrer Instance verbunden sind, geben Sie den folgenden Befehl ein, um sich mit Ihrer Aurora-Datenbank zu verbinden. Ersetzen Sie *DatabaseEndPoint* durch die Endpunktadresse Ihrer Aurora-Datenbank und ersetzen Sie *Port* durch den Port Ihrer Datenbank. Ersetzen Sie *MyUserName* durch den Namen des Benutzers, den Sie beim Erstellen der Datenbank eingegeben haben.

```
mysql -h DatabaseEndpoint -P Port -u MyUserName -p
```

Sie sollten eine Antwort ähnlich der folgenden sehen, die bestätigt, dass Ihre Instance auf Ihre Aurora-Datenbank zugreifen und eine Verbindung mit dieser herstellen kann.

```
bitnami@ip-            $ mysql -h database.cluster-            .us-west-2.rds.amazonaws.
com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 215
Server version: 5.6.10 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Wenn Sie diese Antwort nicht sehen oder eine Fehlermeldung angezeigt wird, müssen Sie möglicherweise die Sicherheitsgruppe Ihrer Datenbank so konfigurieren, dass die private IP-Adresse Ihrer Lightsail-Instance zulässig ist, um damit eine Verbindung herzustellen. Weitere Informationen finden Sie im Abschnitt Konfigurieren der Sicherheitsgruppe für Ihre Aurora-Datenbank dieses Handbuchs.

Schritt 4: Übertragen der MariaDB-Datenbank von Ihrer LAMP-Instance zu Ihrer Aurora-Datenbank

Nachdem Sie nun bestätigt haben, dass Sie von Ihrer Instance aus eine Verbindung zu Ihrer Datenbank herstellen können, sollten Sie die Daten von Ihrer LAMP-Instance-Datenbank zu Ihrer Aurora-Datenbank migrieren. Weitere Informationen finden Sie unter Verwalten eines Amazon-Aurora-MySQL-DB-Clusters im Amazon Aurora-Benutzerhandbuch.

Schritt 5: Konfigurieren Ihrer Anwendung zum Herstellen einer Verbindung mit Ihrer von Aurora verwalteten Datenbank

Nach Übermittlung Ihrer Anwendungsdaten an Ihre Aurora-Datenbank sollten Sie die Anwendung konfigurieren, die auf Ihrer LAMP-Instance ausgeführt wird, um eine Verbindung zu Ihrer Aurora-Datenbank herzustellen. Stellen Sie mithilfe von SSH Connect eine Verbindung zu Ihrer LAMP-Instance her und greifen Sie auf die Datenbankkonfigurationsdatei der Anwendung zu. Definieren Sie in der Konfigurationsdatei die Endpunktadresse Ihrer Aurora-Datenbank, den Datenbankbenutzernamen und das zugehörige Passwort. Folgendes ist ein Beispiel für den Inhalt einer Konfigurationsdatei:

```
bitnami@ip-            :~/htdocs$ cat connectvalues.php
<?php
$host           = 'database.cluster-           .us-west-2.rds.amazonaws.com';
$username       = 'admin';
$password       = 'Password1';
```

Praktische Anleitung: So erstellen Sie eine HAR-Datei

Wenn Sie Probleme mit der Amazon Lightsail-Konsole oder einem Virtual Private Server (VPS) für Lightsail haben, fordert der AWS Support Sie möglicherweise auf, eine HAR-Datei über Ihren Webbrowser abzusenden. Eine HAR-Datei enthält wichtige Informationen, mit denen häufig auftretende und schwer zu diagnostizierende Probleme behoben werden können. Die HAR-Datei ermöglicht es dem AWS Support auch, diese Probleme zu untersuchen oder nachzustellen.

> **Important**
>
> In HAR-Dateien können vertrauliche Informationen wie Benutzernamen, Passwörter und Schlüssel erfasst werden. Stellen Sie sicher, dass Sie alle vertraulichen Informationen aus einer HAR-Datei entfernen, bevor Sie sie teilen.

In diesem Handbuch erfahren Sie, wie Sie eine HAR-Datei in Ihrem Webbrowser erstellen. Eine HTTP-Archivdatei (HAR) ist eine JSON-Datei, die die letzte von Ihrem Browser aufgezeichnete Netzwerkaktivität enthält. Folgen Sie dieser schrittweisen Anleitung, um eine HAR-Datei zu erstellen.

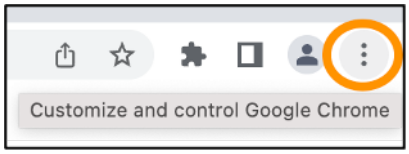
Inhalt

Schritt 1: HAR-Datei in Ihrem Browser erstellen

> **Note**
>
> Diese Anweisungen wurden zuletzt in Google Chrome Version 101.0.4951.64, Microsoft Edge (Chromium) Version 101.0.1210.47 und Mozilla Firefox Version 91.9 getestet. Da es sich bei diesen Browsern um Produkte von Drittanbietern handelt, entsprechen diese Anweisungen möglicherweise nicht der Erfahrung in den neuesten Versionen oder in der von Ihnen verwendeten Version. In einem anderen Browser, wie z. B. dem älteren Microsoft Edge (EdgeHTML) oder Apple Safari für MacOS, ist der Prozess zum Generieren einer HAR-Datei möglicherweise ähnlich, die Schritte sind jedoch unterschiedlich.

Google Chrome

1. Wählen Sie im Browser oben rechts die Option Customize and control Google Chrome (Google Chrome anpassen und einstellen) aus.



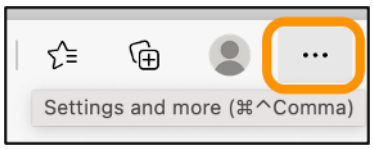
2. Bewegen Sie den Mauszeiger auf More tools (Weitere Tools) und wählen Sie dann Developer tools (Entwicklertools) aus.
3. Wenn DevTools im Browser geöffnet sind, wählen Sie den Bereich Network (Netzwerk).
4. Aktivieren Sie das Kontrollkästchen Preserve log (Protokoll beibehalten).
5. Wählen Sie Clear (Löschen), um alle aktuellen Netzwerkanfragen zu löschen.
6. Reproduzieren Sie das Problem, das bei Ihnen auftritt.

7. Öffnen Sie mit der rechten Maustaste in DevTools das Kontextmenü zu einer beliebigen Netzwerkanforderung.
8. Wählen Sie Save all as HAR with content (Alles als HAR mit Inhalt speichern) aus und speichern Sie dann die Datei.

Weitere Informationen finden Sie unter Open Chrome DevTools und Save all network requests to a HAR file auf der Google Developers-Website.

Microsoft Edge (Chromium)

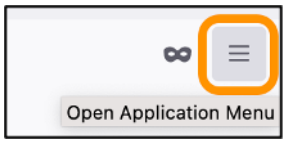
1. Wählen Sie im Browser oben rechts Settings and more (Einstellungen und mehr).



2. Bewegen Sie den Mauszeiger auf More tools (Weitere Tools) und wählen Sie dann Developer tools (Entwicklertools) aus.
3. Wenn DevTools im Browser geöffnet sind, wählen Sie den Bereich Network (Netzwerk).
4. Aktivieren Sie das Kontrollkästchen Preserve log (Protokoll beibehalten).
5. Wählen Sie Clear (Löschen), um alle aktuellen Netzwerkanfragen zu löschen.
6. Reproduzieren Sie das Problem, das bei Ihnen auftritt.
7. Öffnen Sie mit der rechten Maustaste in DevTools das Kontextmenü zu einer beliebigen Netzwerkanforderung.
8. Wählen Sie Save all as HAR with content (Alles als HAR mit Inhalt speichern) aus und speichern Sie dann die Datei.

Mozilla Firefox

1. Wählen Sie im Browser oben rechts die Option Open Application Menu (Anwendungsmenü öffnen).



2. Wählen Sie More tools (Weitere Werkzeuge) und dann Web Developer Tools (Werkzeuge für Webentwickler) aus.

3. Wählen Sie im Menü Web Developer (Webentwickler) die Option Network (Netzwerk). (In einigen Versionen von Firefox befindet sich das Menü Web Developer (Webentwickler) im Menü Tools (Werkzeuge).)
4. Wählen Sie das Zahnradsymbol und dann Persist Logs (Logs nicht leeren) aus.
5. Wählen Sie das Mülleimersymbol Clear (Löschen) aus, um alle aktuellen Netzwerkanforderungen zu löschen.
6. Stellen Sie das Problem nach, das bei Ihnen auftritt.
7. Öffnen Sie mit der rechten Maustaste das Kontextmenü (rechte Maustaste) für einer beliebigen Netzwerkanforderung in der Anforderungsliste.
8. Wählen Sie Save All As HAR (Alles als HAR speichern) aus und speichern Sie dann die Datei.

Schritt 2: HAR-Datei bearbeiten, um vertrauliche Informationen zu entfernen

1. Öffnen Sie die HAR-Datei in einer Texteditoranwendung.
2. Verwenden Sie die Tools „Find“ (Suchen) und „Replace (Ersetzen) des Texteditors, um alle in der HAR-Datei erfassten vertraulichen Informationen zu identifizieren und zu ersetzen. Dazu gehören alle Benutzernamen, Passwörter und Schlüssel, die Sie bei der Erstellung der Datei in Ihren Browser eingegeben haben.
3. Speichern Sie die bearbeitete HAR-Datei, aus der die vertraulichen Informationen entfernt wurden.

Schritt 3: HAR-Datei zur Überprüfung absenden

1. Wählen Sie in der AWS Support Center Console unter Offene Supportfälle Ihren Supportfall aus.
2. Wählen Sie in Ihrem Support-Fall Ihre bevorzugte Kontaktoption, fügen Sie die bearbeitete HAR-Datei an und senden Sie sie dann ab.

Stoppen Ihrer Lightsail-Instance erzwingen

In seltenen Fällen kann eine Instance im `Stopping`-Status hängen bleiben. In diesem Fall liegt möglicherweise ein Problem mit der zugrunde liegenden Hardware vor, die Ihre Lightsail-Instance hostet. In dieser Anleitung erfahren Sie, wie Sie das Stoppen einer Instance erzwingen können, die im `stopping`-Status hängengeblieben ist. Weitere Informationen zum Instance-Status finden Sie unter Starten, Stoppen oder Neustarten Ihrer Amazon Lightsail-Instance.

So erzwingen Sie das Stoppen einer Instance

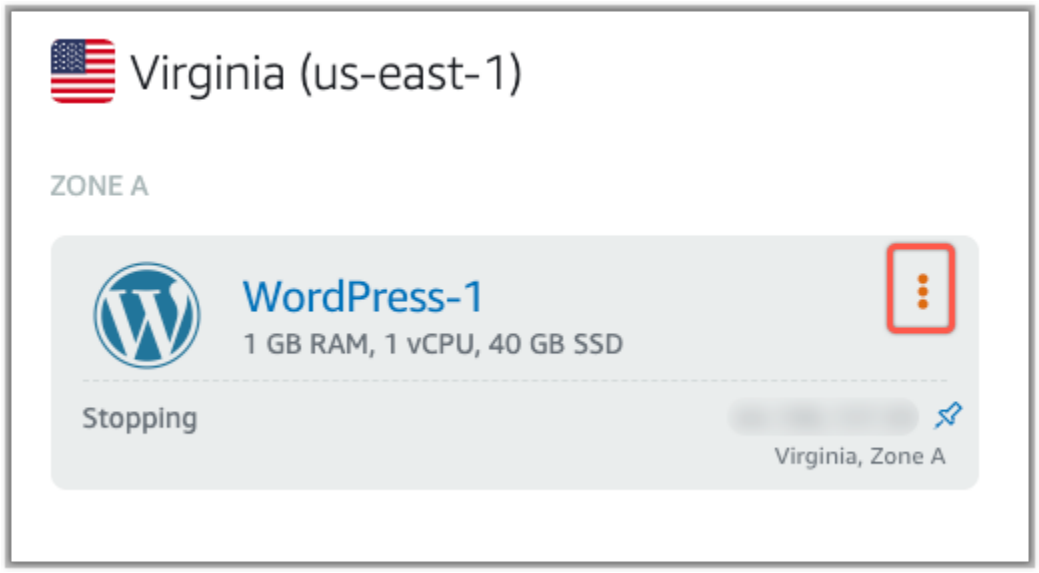
Sie können die Lightsail-Konsole verwenden, um das Stoppen Ihrer Instance zu erzwingen, aber nur, während sich die Instance im Status `stopping` befindet. Alternativ können Sie die AWS Command Line Interface (AWS CLI) verwenden, um das Stoppen einer Instance zu erzwingen, während sich die Instance in einem beliebigen Status außer `shutting-down` und `terminated` befindet. Ein erzwungener Stopp kann einige Minuten in Anspruch nehmen. Wenn die Instance nach 10 Minuten nicht beendet wurde, erzwingen Sie erneut einen Stopp.

Wenn das Stoppen einer Instance erzwungen wird, erhält sie keine Gelegenheit, die Caches oder Metadaten des Dateisystems zu löschen. Nachdem Sie das Stoppen einer Instance erzwungen haben, sollten Sie Dateisystemprüfungen und Reparaturverfahren durchführen.

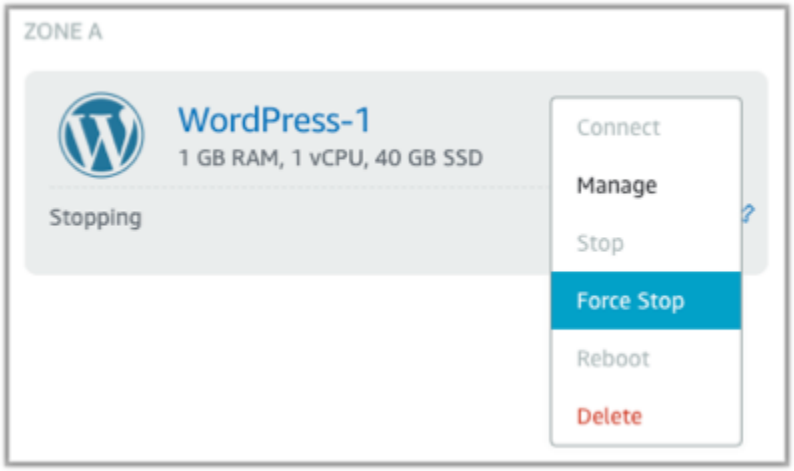
Im folgenden Verfahren werden die verschiedenen Möglichkeiten erläutert, wie Sie das Stoppen einer Lightsail-Instance erzwingen können.

Stoppen einer Instance in der Lightsail-Konsole erzwingen

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie die Registerkarte Instances aus.
3. Suchen Sie die Instance, die im Status `Stopping` hängengeblieben ist. Wählen Sie dann das Aktionsmenüsymbol (⋮), das neben dem Instance-Namen angezeigt wird.



4. Wählen Sie in der angezeigten Dropdown-Liste die Option Stopp erzwingen aus.



Alternativ können Sie den Instance-Namen wählen, um auf die Instance-Verwaltungsseite zuzugreifen. Wählen Sie dann die Schaltfläche Stopp erzwingen.

Stoppen einer Instance mit der AWS CLI erzwingen

1. Bevor Sie beginnen, müssen Sie die AWS CLI installieren. Weitere Informationen finden Sie unter Installieren der AWS Command Line Interface. Stellen Sie sicher, dass Sie die AWS CLI konfigurieren nach der Installation.
2. Verwenden Sie den Befehl stop-instances und den Parameter `--force` wie folgt:

   ```
   aws lightsail stop-instance --instance-name Wordpress-1 --force
   ```

Tutorial: Installieren von Prometheus auf einer Linux-basierten Lightsail-Instance

Prometheus ist ein Open-Source-Zeitreihenüberwachungstool zur Verwaltung einer Vielzahl von Systemressourcen und Anwendungen. Es bietet ein mehrdimensionales Datenmodell, die Möglichkeit, die gesammelten Daten abzufragen, sowie detaillierte Berichte und Datenvisualisierung über Grafana.

Standardmäßig ist Prometheus aktiviert, um Metriken auf dem Server, auf dem es installiert ist, zu sammeln. Mithilfe von Node-Exportern können Metriken aus anderen Ressourcen, wie Webservern, Containern, Datenbanken, benutzerdefinierten Anwendungen und anderen Systemen von Drittanbietern, gesammelt werden. In diesem Tutorial zeigen wir Ihnen, wie Sie Prometheus mit Node-Exportern auf einer Lightsail-Instance installieren und konfigurieren. Eine vollständige Liste der verfügbaren Exporter finden Sie unter Exporter und Integrationen in der Promethe-Dokumentation.

Inhalt

Schritt 1: Erfüllen der Voraussetzungen

Bevor Sie Prometheus auf einer Amazon Lightsail-Instance installieren können, müssen Sie die folgenden Schritte ausführen:

- Erstellen Sie eine Instance inLightsail. Wir empfehlen, den Blueprint Ubuntu 20.04 LTS für Ihre Instance zu verwenden. Weitere Informationen finden Sie unter Erstellen einer Instance in Amazon Lightsail.
- Erstellen Sie eine statische IP-Adresse und fügen Sie diese an Ihre neue Instance an. Weitere Informationen finden Sie unter Erstellen einer statischen IP-Adresse in Amazon Lightsail.

- Öffnen Sie die Ports 9090 und 9100 auf der Firewall Ihrer neuen Instance. Prometheus setzt voraus, dass die Ports 9090 und 9100 geöffnet sind. Weitere Informationen finden Sie unter Hinzufügen und Bearbeiten von Instance-Firewallregeln in Amazon Lightsail.

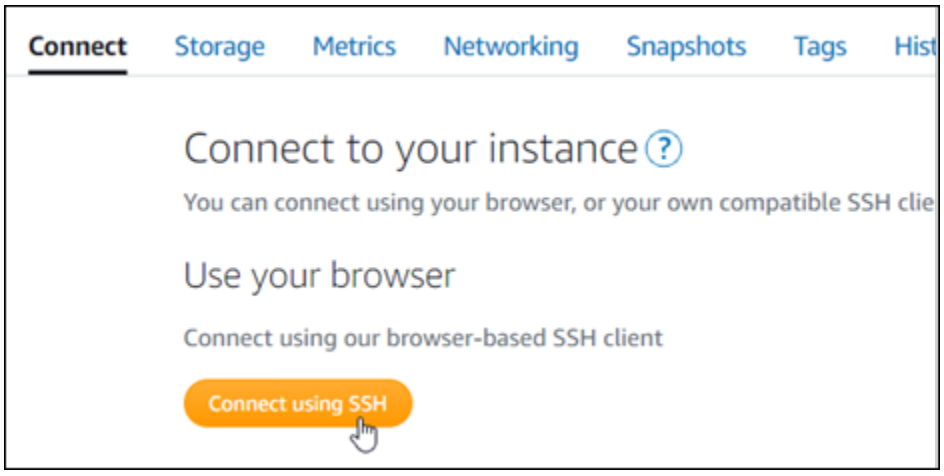
Schritt 2: Benutzer und lokale Systemverzeichnisse zu Ihrer Lightsail-Instance hinzufügen

Führen Sie die folgenden Schritte aus, um eine Verbindung zwischen Ihrer Lightsail-Instance und SSH herzustellen und Benutzer und Systemverzeichnisse hinzuzufügen. Dieses Verfahren erstellt die folgenden Linux-Benutzerkonten:

- `prometheus` – Dieses Konto wird für die Installation und Konfiguration der Serverumgebung verwendet.
- `exporter` – Dieses Konto wird verwendet, um die `node_exporter`-Erweiterung zu konfigurieren.

Diese Benutzerkonten werden ausschließlich zu Verwaltungszwecken erstellt und erfordern daher keine zusätzlichen Benutzerservices oder Berechtigungen, die über den Rahmen dieser Einrichtung hinausgehen. In diesem Verfahren erstellen Sie auch Verzeichnisse zum Speichern und Verwalten der Dateien, Serviceeinsteinstellungen und Daten, die Prometheus zur Überwachung von Ressourcen verwendet.

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie auf Ihrer Instance-Verwaltungsseite unter der Registerkarte Connect (Verbinden) die Option Connect using SSH (Verbinden mit SSH).



3. Nachdem Sie verbunden sind, geben Sie nacheinander die folgenden Befehle ein, um zwei Linux-Benutzerkonten zu erstellen, `prometheus` und `exporter`.

```
sudo useradd --no-create-home --shell /bin/false prometheus
```

```
sudo useradd --no-create-home --shell /bin/false exporter
```

4. Geben Sie nacheinander die folgenden Befehle ein, um lokale Systemverzeichnisse zu erstellen.

```
sudo mkdir /etc/prometheus /var/lib/prometheus
```

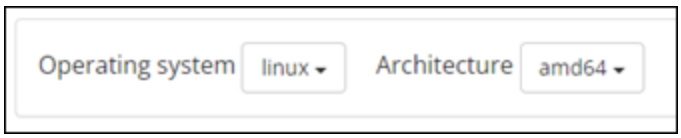
```
sudo chown prometheus:prometheus /etc/prometheus
```

```
sudo chown prometheus:prometheus /var/lib/prometheus
```

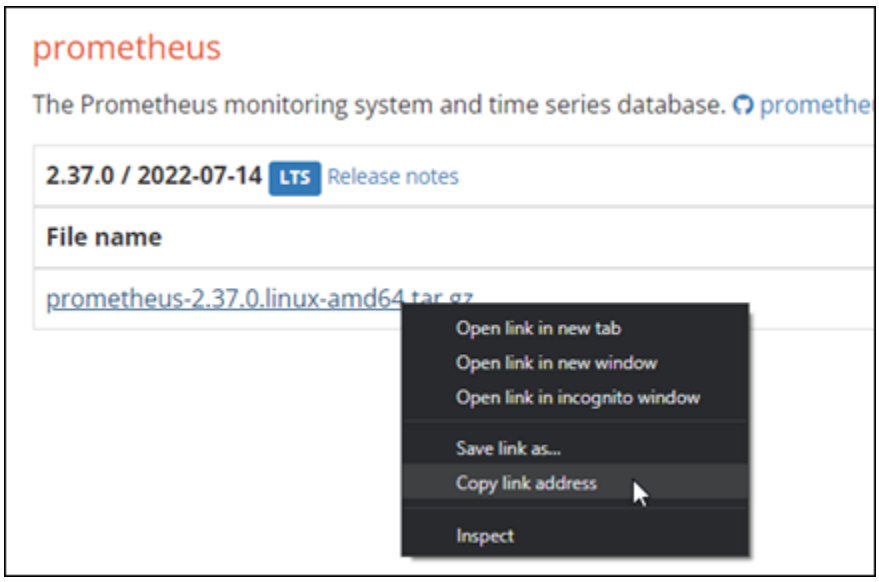
Schritt 3: Die Prometheus-binärpakete herunterladen

Führen Sie die folgenden Schritte aus, um die Prometheus-Binärpakete auf Ihre Lightsail-Instance herunterzuladen.

1. Öffnen Sie einen Webbrowser auf Ihrem lokalen Computer und navigieren Sie zur Promethethe-Downloadseite.
2. Oben auf der Seite wählen Sie im Dropdown-Menü Operating System (Betriebssystem) Linux aus. Wählen Sie für Architecture (Architektur) die Option amd64 aus.



3. Wählen Sie per Eingabetaste oder Rechtsklick den Prometheus-Downloadlink aus, der angezeigt wird, und kopieren Sie die Linkadresse in eine Textdatei auf Ihrem Computer. Tun Sie dasselbe für den node_exporter-Downloadlink, der angezeigt wird. Sie werden später in diesem Verfahren beide kopierten Adressen verwenden.



4. Stellen Sie per SSH eine Verbindung zu Ihrer Lightsail-Instance her.
5. Geben Sie den folgenden Befehl ein, um zu Ihrem Startverzeichnis zu wechseln.

```
cd ~
```

6. Führen Sie die folgenden Schritte aus, um die Prometheus-Binärpakete auf Ihre Instance herunterzuladen.

```
curl -LO prometheus-download-address
```

Ersetzen Sie *prometheus-download-address* mit der Adresse, die Sie zuvor in diesem Verfahren kopiert haben. Der Befehl sollte wie das folgende Beispiel aussehen, wenn Sie die Adresse hinzufügen.

```
curl -LO https://github.com/prometheus/prometheus/releases/download/v2.37.0/
prometheus-2.37.0.linux-amd64.tar.gz
```

7. Geben Sie den folgenden Befehl ein, um die `node_exporter`-Binärpakete auf Ihre Instance herunterzuladen.

```
curl -LO node_exporter-download-address
```

Ersetzen Sie *node_exporter-download-address* mit der Adresse, die Sie im vorherigen Schritt dieses Verfahrens kopiert haben. Der Befehl sollte wie das folgende Beispiel aussehen, wenn Sie die Adresse hinzufügen.

```
curl -LO https://github.com/prometheus/node_exporter/releases/download/v1.3.1/
node_exporter-1.3.1.linux-amd64.tar.gz
```

8. Führen Sie nacheinander die folgenden Befehle aus, um den Inhalt der heruntergeladenen Prometheus- und Node-Exporter-Dateien zu extrahieren.

```
tar -xvf prometheus-2.37.0.linux-amd64.tar.gz
```

```
tar -xvf node_exporter-1.3.1.linux-amd64.tar.gz
```

Nachdem der Inhalt der heruntergeladenen Dateien extrahiert wurde, werden mehrere Unterverzeichnisse erstellt.

9. Geben Sie nacheinander die folgenden Befehle ein, um die extrahierten `prometheus`- und `promtool`-Dateien in das `/usr/local/bin`-Programmverzeichnis kopieren.

```
sudo cp -p ./prometheus-2.37.0.linux-amd64/prometheus /usr/local/bin
```

```
sudo cp -p ./prometheus-2.37.0.linux-amd64/promtool /usr/local/bin
```

10. Geben Sie den folgenden Befehl ein, um den Besitzstatus der `prometheus`- und `promtool`-Dateien zu dem `prometheus`-Benutzer zu ändern, den Sie zuvor in diesem Tutorial erstellt haben.

```
sudo chown prometheus:prometheus /usr/local/bin/prom*
```

11. Geben Sie nacheinander die folgenden Befehle ein, um die `consoles`- und `console_libraries`-Unterverzeichnisse zu `/etc/prometheus` zu kopieren. Die `-r`-Option führt eine rekursive Kopie aller Verzeichnisse innerhalb der Hierarchie durch.

```
sudo cp -r ./prometheus-2.37.0.linux-amd64/consoles /etc/prometheus
```

```
sudo cp -r ./prometheus-2.37.0.linux-amd64/console_libraries /etc/prometheus
```

12. Geben Sie nacheinander die folgenden Befehle ein, um den Besitzstatus der kopierten Dateien zu dem `prometheus`-Benutzer zu ändern, den Sie zuvor in diesem Tutorial erstellt haben. Die

`-R`-Option führt eine rekursive Besirtzänderung für alle Dateien und Verzeichnisse innerhalb der Hierarchie durch.

```
sudo chown -R prometheus:prometheus /etc/prometheus/consoles
```

```
sudo chown -R prometheus:prometheus /etc/prometheus/console_libraries
```

13. Geben Sie nacheinander die folgenden Befehle ein, um die Konfigurationsdatei `prometheus.yml` in das `/etc/prometheus`-Verzeichnis zu kopiere und den Besitzstatus der kopierten Datei zu dem `prometheus`-Benutzer zu ändern, den Sie zuvor in diesem Tutorial erstellt haben.

```
sudo cp -p ./prometheus-2.37.0.linux-amd64/prometheus.yml /etc/prometheus
```

```
sudo chown prometheus:prometheus /etc/prometheus/prometheus.yml
```

14. Geben Sie den folgenden Befehl ein, um die `node_exporter`-Datei aus dem `./node_exporter*`-Unterverzeichnis in das `/usr/local/bin`-Programmverzeichnis zu kopieren.

```
sudo cp -p ./node_exporter-1.3.1.linux-amd64/node_exporter /usr/local/bin
```

15. Geben Sie den folgenden Befehl ein, um den Besitzstatus der Datei zu dem `exporter`-Benutzer zu ändern, den Sie zuvor in diesem Tutorial erstellt haben.

```
sudo chown exporter:exporter /usr/local/bin/node_exporter
```

Schritt 4: Prometheus konfigurieren

Führen Sie das folgende Verfahren durch, um Prometheus zu konfigurieren. In diesem Verfahren öffnen und bearbeiten Sie die `prometheus.yml`-Datei, die verschiedene Einstellungen für das Prometheus-Tool enthält. Prometheus richtet basierend auf den Einstellungen, die Sie in der Datei konfigurieren, eine Überwachungsumgebung ein.

1. Stellen Sie per SSH eine Verbindung zu Ihrer Lightsail-Instance her.
2. Geben Sie den folgenden Befehl ein, um eine Sicherungskopie der `prometheus.yml`-Datei zu erstellen, bevor Sie sie öffnen und bearbeiten.

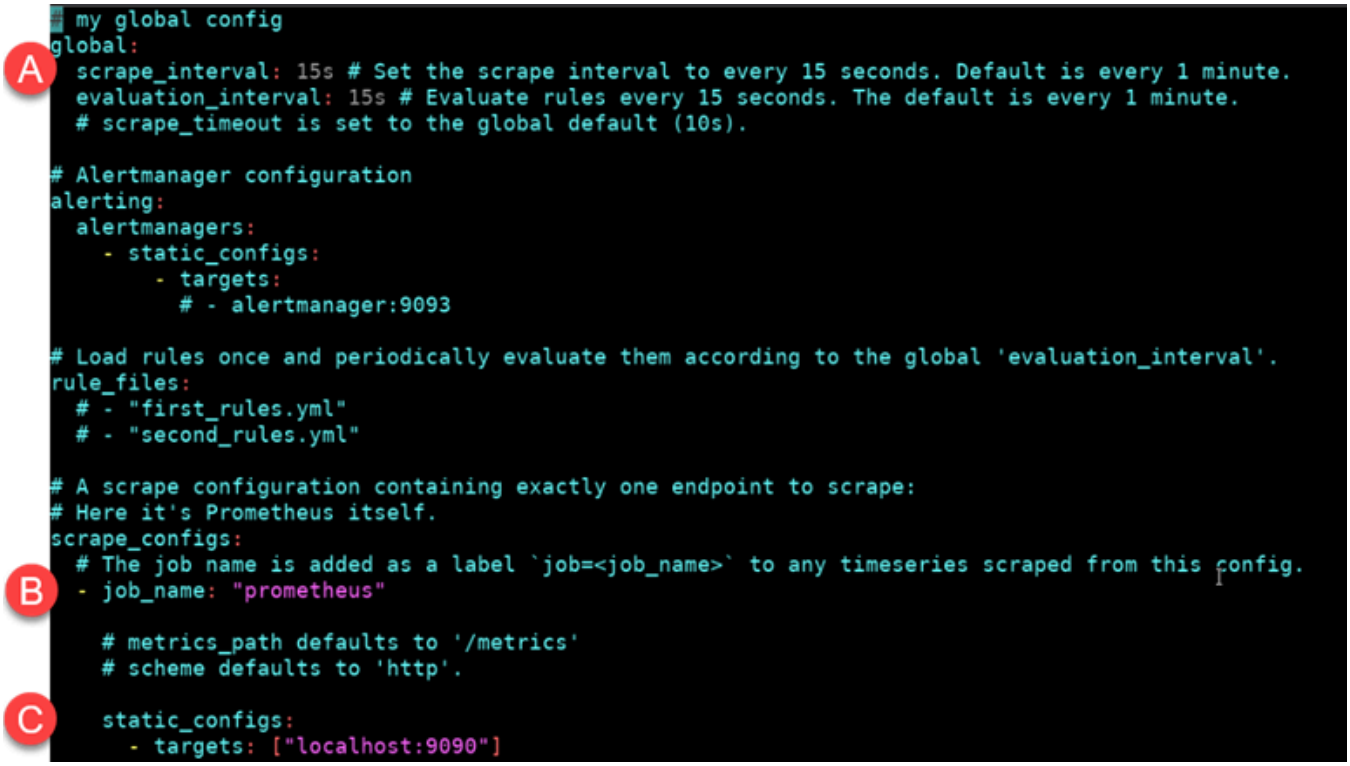
```
sudo cp /etc/prometheus/prometheus.yml /etc/prometheus/prometheus.yml.backup
```

3. Geben Sie den folgenden Befehl ein, um die `prometheus.yml`Datei mit Vim zu öffnen.

```
sudo vim /etc/prometheus/prometheus.yml
```

Im Folgenden finden Sie einige wichtige Parameter, die Sie möglicherweise in der `prometheus.yml`-Datei konfigurieren möchten:

- `scrape_interval` – Dieser Parameter unter dem `global`-Header definiert das Zeitintervall (in Sekunden) dafür, wie oft Prometheus oder Metrikdaten für ein bestimmtes Ziel sammeln oder scrapen wird. Wie durch das `global`-Tag angegeben, ist diese Einstellung universell für alle Ressourcen, die Prometheus überwacht. Diese Einstellung gilt auch für Exporter, es sei denn, ein einzelner Exporter stellt einen anderen Wert bereit, der den globalen Wert außer Kraft setzt. Sie können diesen Parameter auf dem aktuellen Wert von 15 Sekunden belassen.
- `job_name` – Dieser Parameter unter dem `scrape_configs`-Header ist ein Label, das Exporter in der Ergebnismenge einer Datenabfrage oder visuellen Anzeige identifiziert. Sie können den Wert eines Auftragsnamens angeben, um die Ressourcen, die in Ihrer Umgebung überwacht werden, am besten widerzuspiegeln. Beispielsweise können Sie einen Auftrag für die Verwaltung einer Website als `business-web-app` kennzeichnen, oder Sie können eine Datenbank als `mysql-db-1` kennzeichnen. In diesem ersten Setup überwachen Sie nur den Prometheus-Server, sodass Sie den aktuellen `prometheus`-Wert behalten können.
- `targets` – Die `targets`-Einstellung unter dem `static_configs`-Header verwendet ein `ip_addr:port`-Schlüssel-Wert-Paar zur Identifizierung des Speicherorts, an dem ein bestimmter Exporter ausgeführt wird. Sie werden die Standardeinstellung in Schritt 4–7 dieses Verfahrens ändern.



> **Note**
>
> Für diese Ersteinrichtung müssen Sie nicht die `alerting`-und `rule_files`-Parameter konfigurieren.

4. In der `prometheus.yml`-Datei, die Sie in Vim geöffnet haben, drücken Sie die I-Taste, um den Einfügemodus in Vim zu starten.
5. Scrollen Sie zum `targets`-Parameter, der sich unter dem `static_configs`-Header befindet.
6. Ändern Sie die Standardeinstellung auf *<ip_addr>*`:9090`. Ersetzen Sie *<ip_addr>* mit der statischen IP-Adresse der Instance. Der geänderte Parameter sollte wie im folgenden Beispiel aussehen.

```
static_configs:
  - targets: ["192.0.2.0:9090"]
```

7. Drücken Sie die Esc-Taste, um den Eingabemodus zu beenden, und geben Sie :wq! ein, um Ihre Änderungen zu speichern und Vim zu verlassen.

8. (Optional) Wenn etwas schief gelaufen ist, geben Sie den folgenden Befehl ein, um die `prometheus.yml`-Datei mit dem Backup, das Sie zuvor in diesem Verfahren erstellt haben, zu ersetzen.

```
sudo cp /etc/prometheus/prometheus.yml.backup /etc/prometheus/prometheus.yml
```

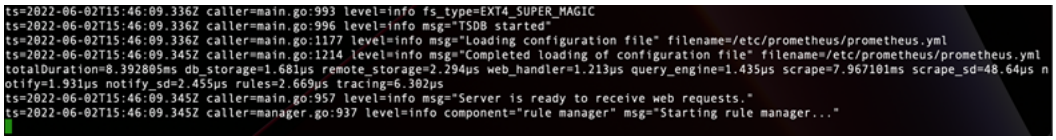
Schritt 5: Prometheus starten

Führen Sie die folgenden Schritte aus, um den Prometheus-Service auf Ihrer Instance zu starten.

1. Stellen Sie per SSH eine Verbindung zu Ihrer Lightsail-Instance her.
2. Geben Sie den folgenden Befehl ein, um den Prometheus-Service zu starten.

```
sudo -u prometheus /usr/local/bin/prometheus --config.file /etc/prometheus/
prometheus.yml --storage.tsdb.path /var/lib/prometheus --web.console.templates=/
etc/prometheus/consoles --web.console.libraries=/etc/prometheus/console_libraries
```

Die Befehlszeile gibt Details zum Startvorgang und anderen Services aus. Es sollte auch darauf hinweisen, dass der Service auf Port 9090 zuhört.



Wenn der Service nicht startet, finden Sie im Abschnitt Schritt 1: Erfüllen der Voraussetzungen in diesem Tutorial Informationen zum Erstellen von Instance-Firewall-Regeln, um Datenverkehr auf diesem Port zuzulassen. Gehen Sie für andere Fehler die `prometheus.yml`-Datei durch, um zu bestätigen, dass keine Syntaxfehler vorliegen.

3. Nachdem der ausgeführte Service validiert wurde, drücken Sie Strg+C, um ihn zu beenden.
4. Geben Sie den folgenden Befehl ein, um die `systemd`-Konfigurationsdatei in Vim zu öffnen. Mit dieser Datei wird Prometheus gestartet.

```
sudo vim /etc/systemd/system/prometheus.service
```

5. Fügen Sie die folgenden Zeilen in die Datei ein.

```
[Unit]
Description=PromServer
```

```
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
--config.file /etc/prometheus/prometheus.yml \
--storage.tsdb.path /var/lib/prometheus/ \
--web.console.templates=/etc/prometheus/consoles \
--web.console.libraries=/etc/prometheus/console_libraries

[Install]
WantedBy=multi-user.target
```

Die vorhergehenden Anweisungen werden von dem Linux `systemd` Service Manager verwendet, um Prometheus auf dem Server zu starten. Wenn es aufgerufen wird, läuft Prometheus als der `prometheus`-Benutzer und referenziert die `prometheus.yml`-Datei zum Laden der Konfigurationseinstellungen und Speichern der Zeitreihendaten im `/var/lib/prometheus`-Verzeichnis. Sie können `man systemd` über die Befehlszeile ausführen, um mehr Informationen über den Service zu erhalten.

6. Drücken Sie die Esc-Taste, um den Eingabemodus zu beenden, und geben Sie :wq! ein, um Ihre Änderungen zu speichern und Vim zu verlassen.
7. Geben Sie den folgenden Befehl ein, um die Informationen in den `systemd` Service Manager zu laden.

   ```
   sudo systemctl daemon-reload
   ```

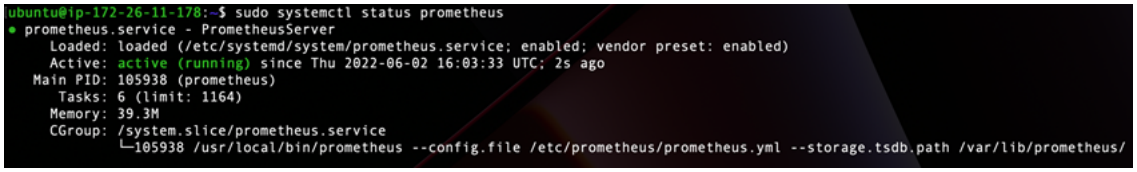
8. Geben Sie den folgenden Befehl ein, um Prometheus neu zu starten.

   ```
   sudo systemctl start prometheus
   ```

9. Geben Sie den folgenden Befehl ein, um den Status des Prometheus-Services zu überprüfen.

   ```
   sudo systemctl status prometheus
   ```

   Wird der Service ordnungsgemäß gestartet, erhalten Sie eine Ausgabe, die der im folgenden Beispiel ähnelt.



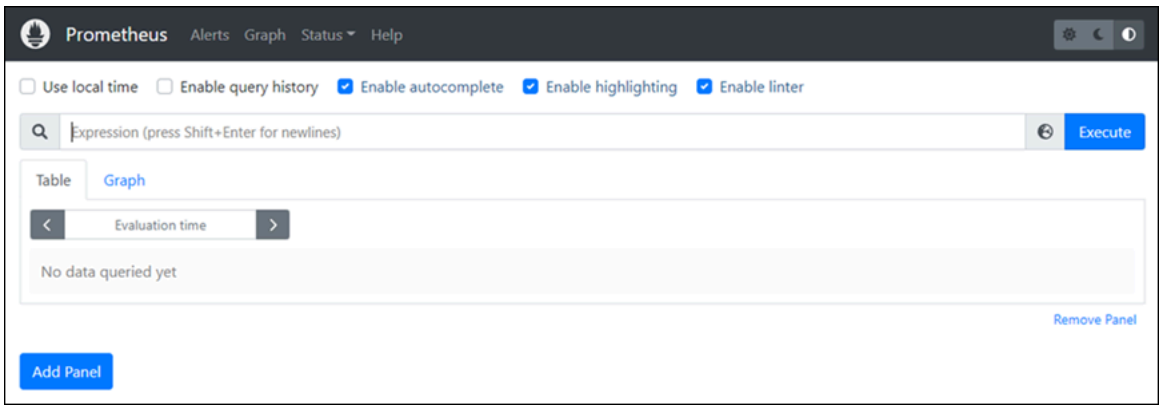
10. Drücken Sie auf Q, um den Status-Befehl zu beenden.
11. Geben Sie den folgenden Befehl ein, damit Prometheus beim Booten der Instance starten kann.

```
sudo systemctl enable prometheus
```

12. Öffnen Sie einen Webbrowser auf Ihrem lokalen Computer und rufen Sie die folgende Webadresse auf, um die Prometheus-Verwaltungsoberfläche anzuzeigen.

```
http:<ip_addr>:9090
```

Stellen Sie sicher, dass Sie *<ip_addr>* mit der statischen IP-Adresse Ihrer Lightsail-Instance ersetzen. Sie sollten ein Dashboard sehen, das dem folgenden Beispiel ähnelt.



Schritt 6: Node Exporter starten

Führen Sie die folgenden Schritte aus, um den Node-Exporter-Service zu starten.

1. Stellen Sie per SSH eine Verbindung zu Ihrer Lightsail-Instance her.
2. Geben Sie den folgenden Befehl ein, um eine `systemd`-Servicedatei für `node_exporter` mit Vim zu erstellen.

```
sudo vim /etc/systemd/system/node_exporter.service
```

3. Drücken Sie die Taste I, um in den Einfügemodus in Vim zu gelangen.

4. Fügen Sie die folgenden Textzeilen der Datei hinzu. Dadurch wird `node_exporter` mit Überwachungskollektoren für CPU-Auslastung, Dateisystemnutzung und Speicherressourcen konfiguriert.

```
[Unit]
Description=NodeExporter
Wants=network-online.target
After=network-online.target

[Service]
User=exporter
Group=exporter
Type=simple
ExecStart=/usr/local/bin/node_exporter --collector.disable-defaults \
--collector.meminfo \
--collector.loadavg \
--collector.filesystem

[Install]
WantedBy=multi-user.target
```

> **Note**
>
> Diese Anweisungen deaktivieren Standardmaschinenmetriken für Node Exporter. Eine vollständige Liste der für Ubuntu verfügbaren Metriken finden Sie unter Prometheus node_exporter man page in der Ubuntu-Dokumentation.

5. Drücken Sie die Esc-Taste, um den Eingabemodus zu beenden, und geben Sie :wq! ein, um Ihre Änderungen zu speichern und Vim zu verlassen.
6. Geben Sie den folgenden Befehl ein, um den `systemd`-Prozess neu zu laden.

```
sudo systemctl daemon-reload
```

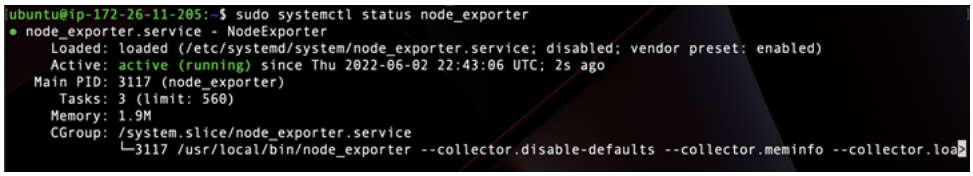
7. Geben Sie den folgenden Befehl ein, um den `node_exporter`-Service zu starten.

```
sudo systemctl start node_exporter
```

8. Geben Sie den folgenden Befehl ein, um den Status des `node_exporter`-Services zu überprüfen.

```
sudo systemctl status node_exporter
```

Wird der Service erfolgreich gestartet, erhalten Sie eine Ausgabe, die der im folgenden Beispiel ähnelt.



9. Drücken Sie auf Q, um den Status-Befehl zu beenden.
10. Geben Sie den folgenden Befehl ein, damit Node Exporter beim Booten der Instance starten kann.

```
sudo systemctl enable node_exporter
```

Schritt 7: Prometheus mit dem Node-Exporter-Datensammler konfigurieren

Führen Sie die folgenden Schritte aus, um Prometheus mit dem Node-Exporter-Datensammler zu konfigurieren. Dafür fügen Sie einen neuen `job_name`-Parameter für `node_exporter` in der `prometheus.yml`-Datei hinzu.

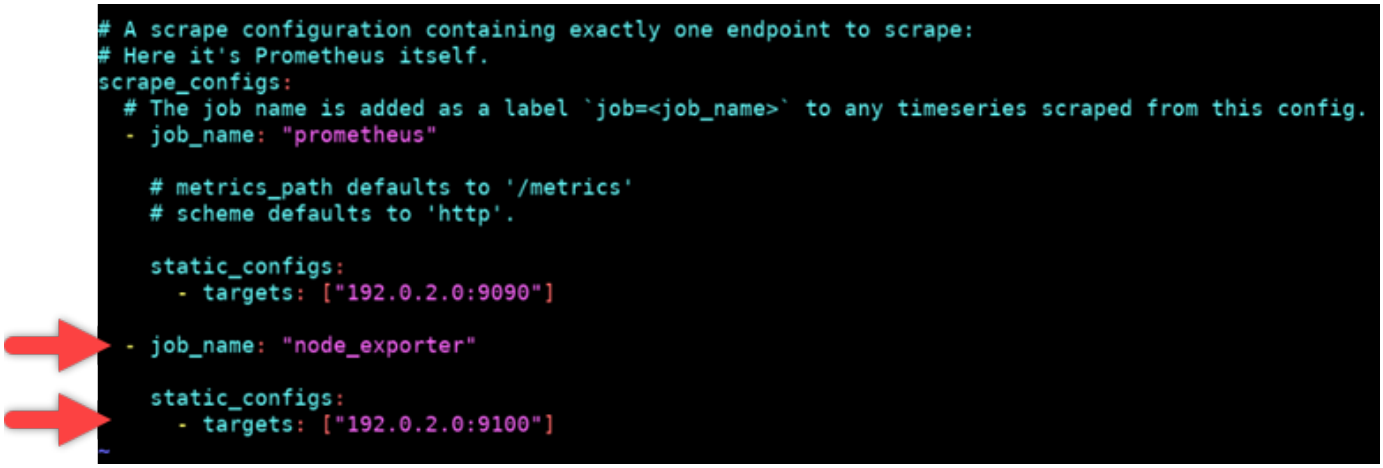
1. Stellen Sie per SSH eine Verbindung zu Ihrer Lightsail-Instance her.
2. Geben Sie den folgenden Befehl ein, um die `prometheus.yml`Datei mit Vim zu öffnen.

```
sudo vim /etc/prometheus/prometheus.yml
```

3. Drücken Sie die Taste I, um in den Einfügemodus in Vim zu gelangen.
4. Fügen Sie unterhalb des vorhandenen `- targets: ["<ip_addr>:9090"]`-Parameters die folgenden Textzeilen in die Datei ein.

```
- job_name: "node_exporter"

static_configs:
- targets: ["<ip_addr>:9100"]
```

Der geänderte Parameter in der `prometheus.yml`-Datei sollte wie im folgenden Beispiel aussehen.



Beachten Sie Folgendes:

- Node Exporter hört zum Scrapen der Daten durch den `prometheus`-Server Port 9100 zu. Vergewissern Sie sich, dass Sie die Schritte zum Erstellen von Instance-Firewall-Regeln, wie im Abschnitt Schritt 1: Erfüllen der Voraussetzungen dieses Tutorials dargelegt, befolgt haben.
- Wie bei der Konfiguration von `prometheus` `job_name` ersetzen Sie *<ip_addr>* mit der statischen IP-Adresse, die an Ihre Lightsail-Instance angefügt ist.

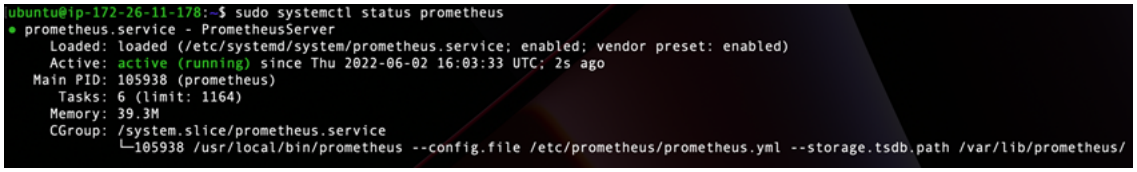
5. Drücken Sie die Esc-Taste, um den Eingabemodus zu beenden, und geben Sie :wq! ein, um Ihre Änderungen zu speichern und Vim zu verlassen.
6. Geben Sie den folgenden Befehl ein, um den Prometheus-Service neu zu starten, damit die Änderungen an der Konfigurationsdatei wirksam werden können.

```
sudo systemctl restart prometheus
```

7. Geben Sie den folgenden Befehl ein, um den Status des Prometheus-Services zu überprüfen.

```
sudo systemctl status prometheus
```

Wird der Service ordnungsgemäß neu gestartet, erhalten Sie eine Ausgabe, die der folgenden ähnelt.

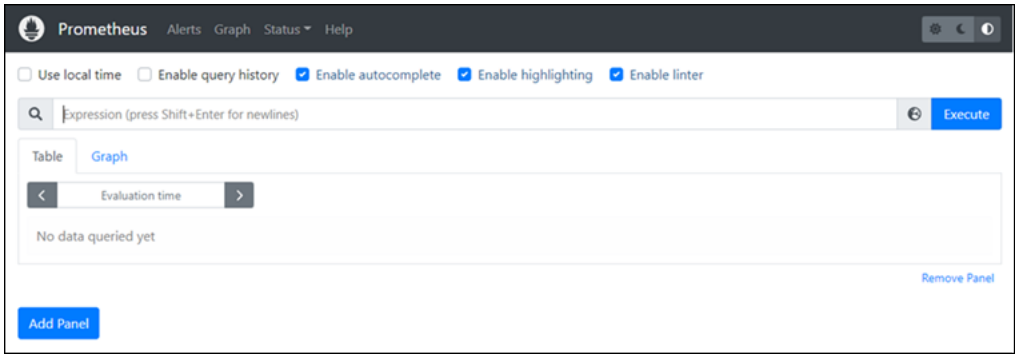


8. Drücken Sie auf Q, um den Status-Befehl zu beenden.

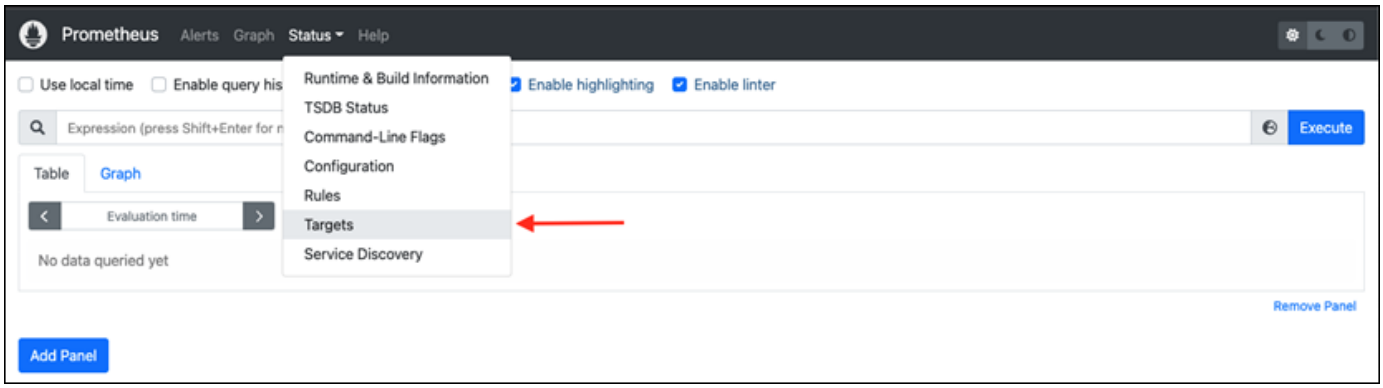
9. Öffnen Sie einen Webbrowser auf Ihrem lokalen Computer und rufen Sie die folgende Webadresse auf, um die Prometheus-Verwaltungsoberfläche anzuzeigen.

```
http:<ip_addr>:9090
```

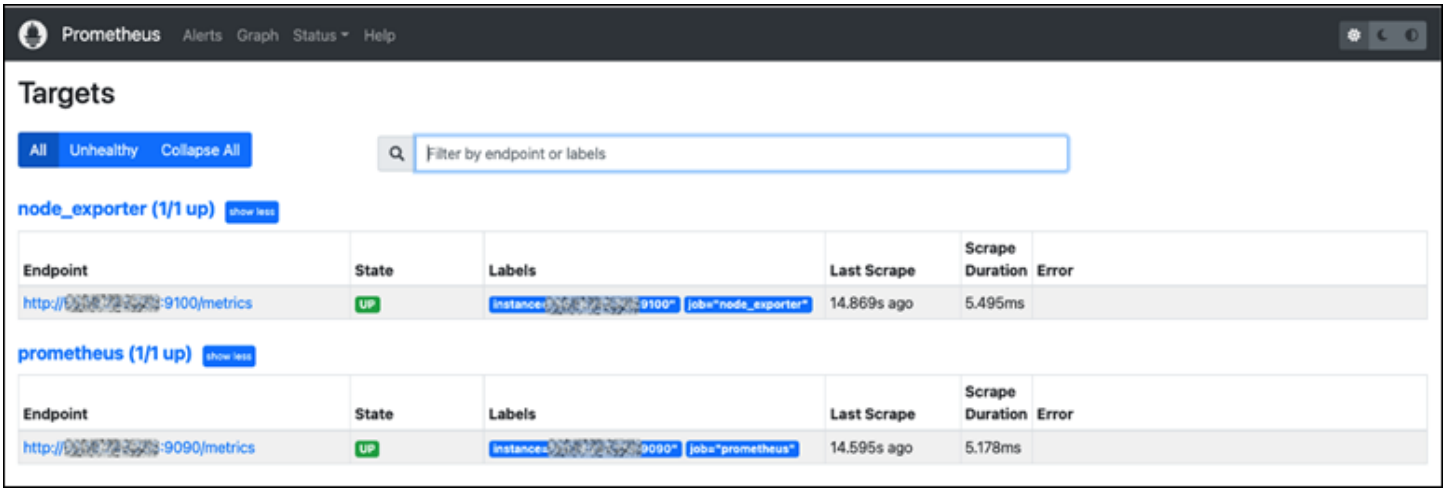
   Stellen Sie sicher, dass Sie *<ip_addr>* mit der statischen IP-Adresse Ihrer Lightsail-Instance ersetzen. Sie sollten ein Dashboard sehen, das dem folgenden Beispiel ähnelt.



10. Wählen Sie im Hauptmenü das Status-Dropdown-Menü und dann Targets (Ziele) aus.



Auf dem nächsten Bildschirm sollten Sie zwei Ziele sehen. Das erste Ziel ist für den node_exporter-Metrik-Kollektorauftrag und das zweite ist für den Prometheus-Auftrag.



Die Umgebung ist jetzt korrekt für das Sammeln von Metriken und die Überwachung des Servers eingerichtet.

Tutorial: Starten und Konfigurieren einer Lightsail-LAMP-Instance

Amazon Lightsail ist der einfachste Weg, um mit Amazon Web Services (AWS) zu beginnen, wenn Sie nur virtuelle private Server benötigen. Lightsail bietet alles, was Sie benötigen, um Ihr Projekt schnell zu starten – eine virtuelle Maschine, SSD-basierten Speicher, Datenübertragung, DNS-Verwaltung und eine statische IP – zu einem niedrigen, vorhersehbaren Preis.

In diesem Tutorial erfahren Sie, wie Sie eine LAMP-Instance auf Lightsail starten und konfigurieren. Es beschreibt die Schritte, um sich über SSH mit Ihrer Instance zu verbinden, das Anwendungspasswort für Ihre Instance zu erhalten, eine statische IP zu erstellen und sie an Ihre Instance anzufügen, und eine DNS-Zone zu erstellen und Ihrer Domain zuzuordnen. Wenn Sie mit diesem Tutorial fertig sind, verfügen Sie über die Grundlagen, um Ihre Instance auf Lightsail zum Laufen zu bringen.

Inhalt

- Nächste Schritte

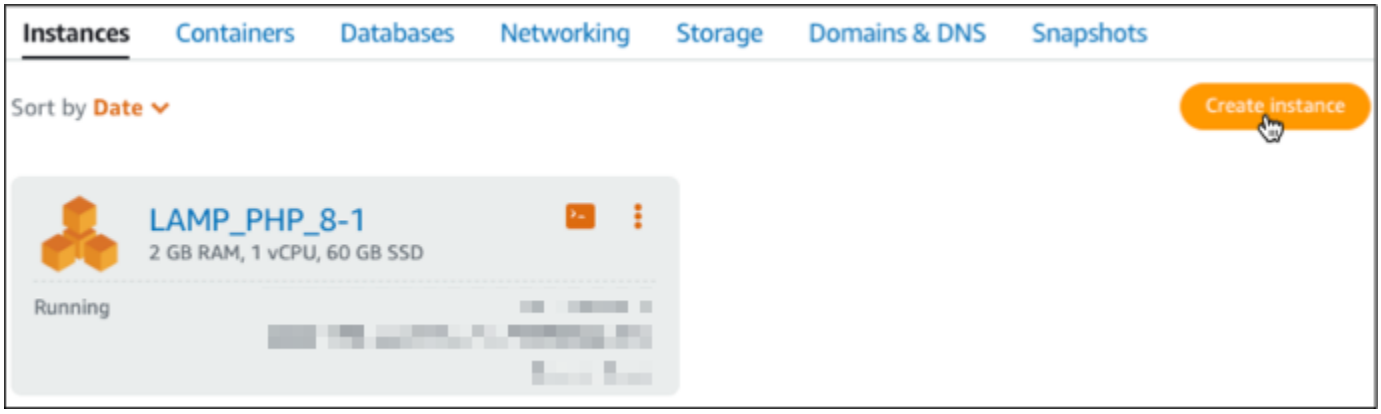
Schritt 1: Registrieren bei AWS

Für dieses Tutorial ist ein - AWS Konto erforderlich. Melden Sie sich bei an oder melden Sie sich bei an AWSAWS, wenn Sie bereits über ein -Konto verfügen.

Schritt 2: Erstellen einer LAMP-Instance

Starten Sie Ihre LAMP-Instance in Lightsail. Weitere Informationen zum Erstellen einer Instance in Lightsail finden Sie unter Erstellen einer Amazon Lightsail-Instance in der Lightsail-Dokumentation.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Registerkarte Instances der Lightsail-Startseite die Option Instance erstellen aus.

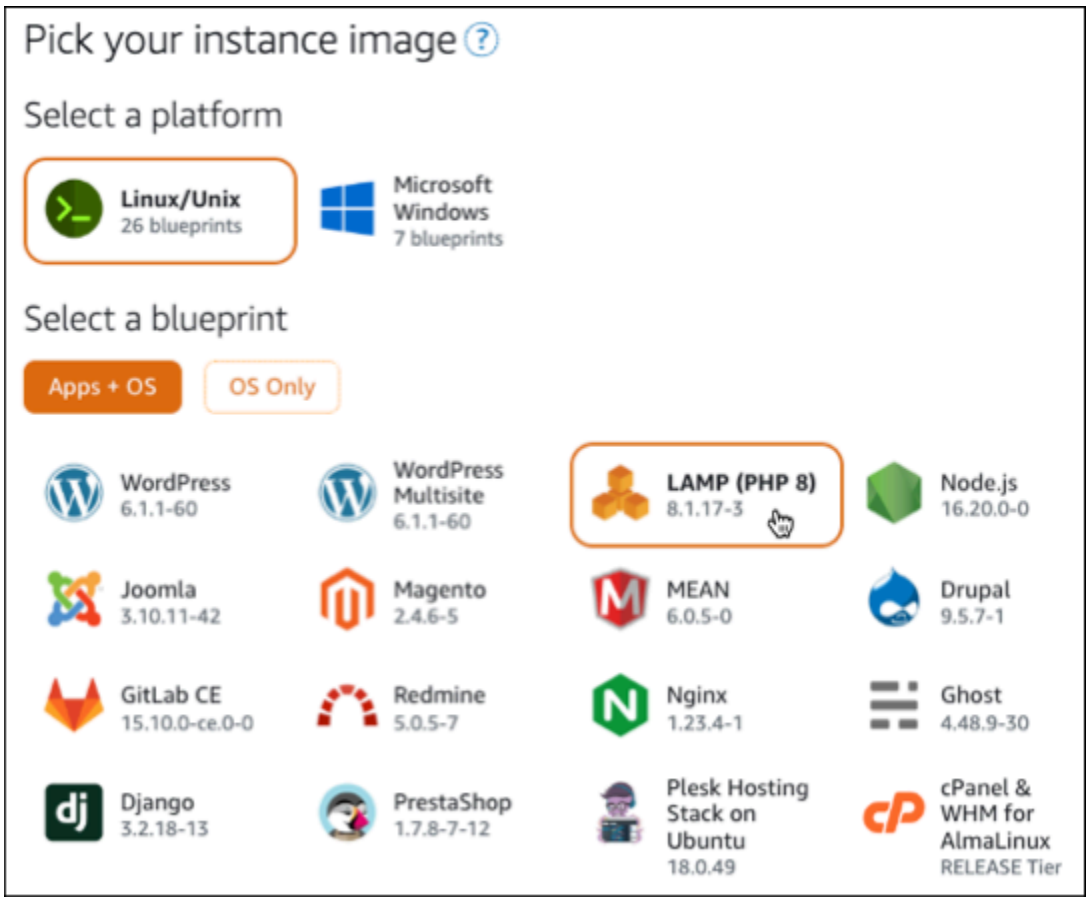


3. Wählen Sie die AWS-Region und Availability Zone für Ihre Instance aus.

4. Wählen Sie Ihr Instance-Image.

   a. Wählen Sie Linux/Unix als Plattform aus.

   b. Wählen Sie LAMP (PHP 8) als Vorlage aus.



5. Wählen Sie einen Instance-Plan.

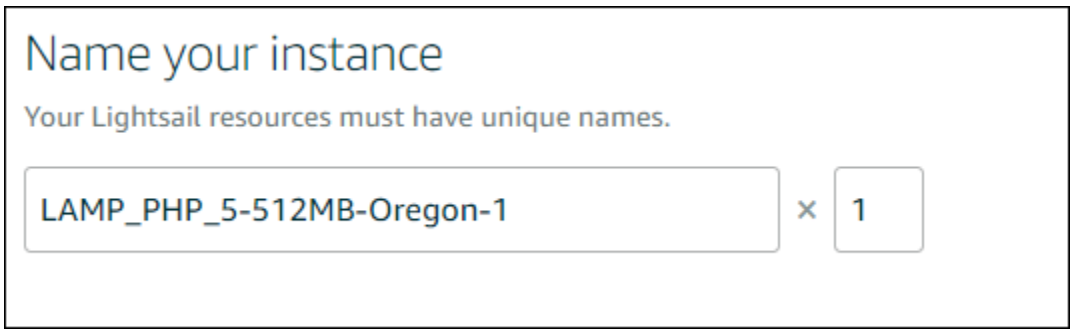
   Ein Plan beinhaltet niedrige, vorhersehbare Kosten, die Maschinenkonfiguration (RAM, SSD, vCPU) und die Zuteilung der Datenübertragung. Sie können den Lightsail-Plan von 3,50 USD für einen Monat (bis zu 750 Stunden) kostenlos testen. AWS erwirbt einen kostenlosen Monat für Ihr Konto.

   > **Note**
   >
   > Im Rahmen des AWS kostenlosen Kontingents für können Sie kostenlos mit Amazon Lightsail für ausgewählte Instance-Pakete beginnen. Weitere Informationen finden Sie unter AWS Kostenloses Kontingent auf der Seite Amazon Lightsail – Preise.

6. Geben Sie einen Namen für Ihre Instance ein.

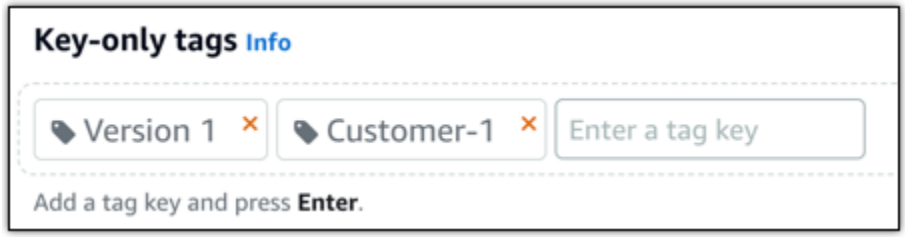
   Ressourcennamen:

- Muss in jedem AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
- Muss zwischen 2 und 255 Zeichen enthalten.
- Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
- Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.



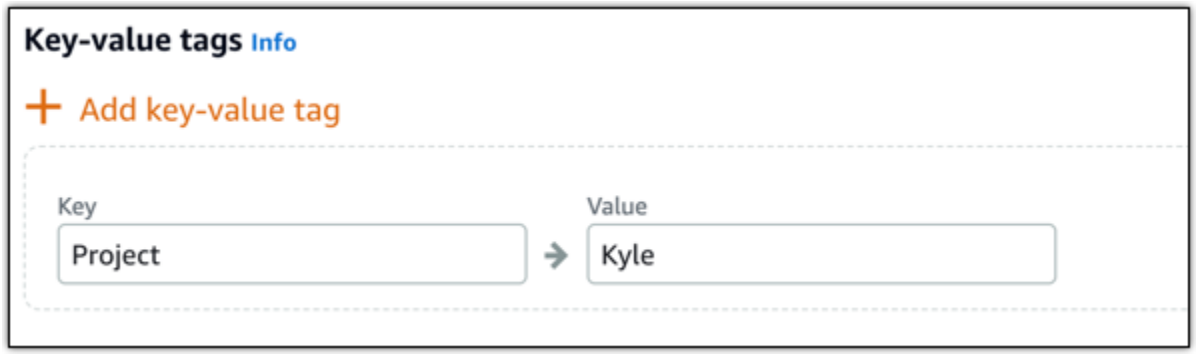
7. Wählen Sie eine der folgenden Optionen, um Ihrer Instance Tags hinzuzufügen:

   - Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.

   - Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

     Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.



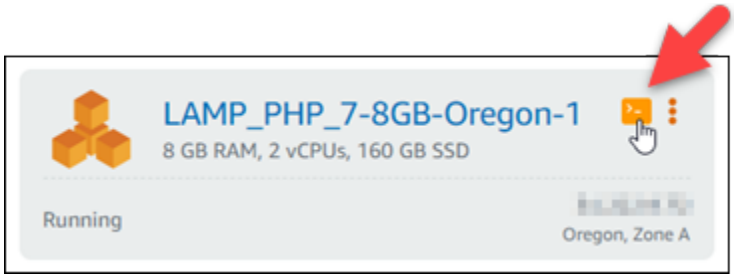
> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

8. Wählen Sie Create instance (Instance erstellen).

Schritt 3: Herstellen einer Verbindung zu Ihrer Instance über SSH und Abrufen des Anwendungspassworts für Ihre LAMP-Instance.

Das Standardpasswort für die Anmeldung an Ihrer Datenbank in LAMP wird in Ihrer Instance gespeichert. Rufen Sie sie ab, indem Sie über das browserbasierte SSH-Terminal in der Lightsail-Konsole eine Verbindung zu Ihrer Instance herstellen und einen speziellen Befehl ausführen. Weitere Informationen finden Sie unter Abrufen des Anwendungsbenutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.

1. Wählen Sie auf der Registerkarte Instances der Lightsail-Startseite das SSH-Schnellverbindungssymbol für Ihre LAMP-Instance aus.



2. Nachdem sich das browserbasierte SSH-Client-Fenster geöffnet hat, geben Sie den folgenden Befehl ein, um das Standard-Anwendungspasswort abzurufen:

```
cat bitnami_application_password
```

> **Note**
>
> Wenn Sie sich in einem anderen Verzeichnis als dem Stammverzeichnis des Benutzers befinden, geben Sie `cat $HOME/bitnami_application_password` ein.

3. Notieren Sie sich das auf dem Bildschirm angezeigte Passwort. Sie benötigen dieses Passwort später, um Bitnami-Anwendungen auf Ihrer Instance zu installieren oder um auf die MySQL-Datenbank mit dem Benutzernamen `root` zuzugreifen.

Schritt 4: Installieren einer Anwendung auf Ihrer LAMP-Instance

Stellen Sie Ihre PHP-Anwendung auf der LAMP-Instance bereit oder installieren Sie eine Bitnami-Anwendung. Das Haupt-Verzeichnis für die Bereitstellung Ihrer PHP-Anwendung ist `/opt/bitnami/apache2/htdocs`. Kopieren Sie Ihre PHP-Anwendungsdateien in dieses Verzeichnis und greifen Sie auf die Anwendung zu, indem Sie nach der öffentlichen IP-Adresse Ihrer Instance suchen.

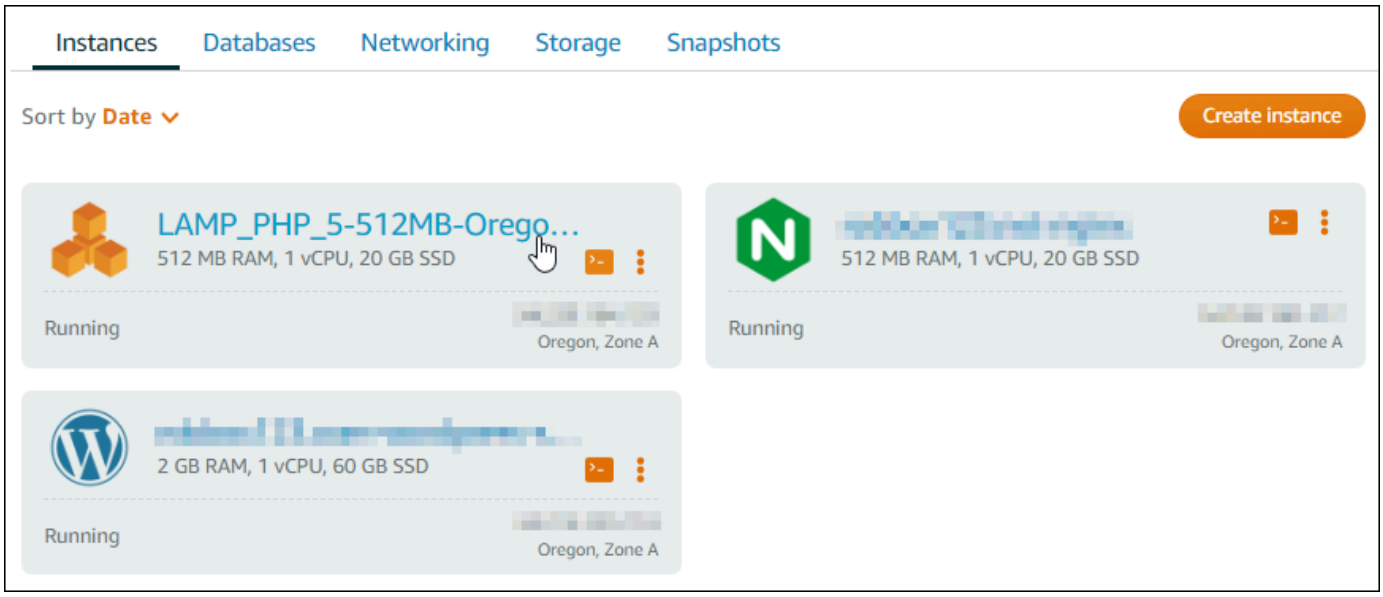
Sie können eine Bitnami Anwendung auch mit den Modul-Installationsprogrammen installieren. Laden Sie WordPress, Drupal, Magento, Moodle und andere Anwendungen von der Bitnami-Website herunter und erweitern Sie die Funktionalität Ihres Servers. Weitere Informationen zum Installieren von Bitnami-Anwendungen finden Sie unter Erste Schritte in der Bitnami-Dokumentation.

Schritt 5: Erstellen einer statischen IP-Adresse und Anfügen der Adresse an Ihre LAMP-instance

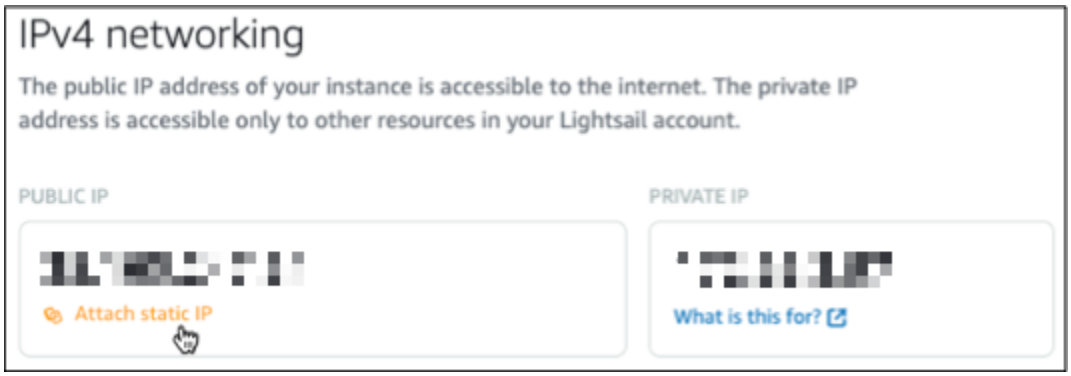
Die standardmäßige öffentliche IP für Ihre LAMP-Instance ändert sich, wenn Sie die Instance stoppen und starten. Eine statische IP-Adresse, die einer Instance zugeordnet ist, bleibt gleich, auch wenn Sie Ihre Instance anhalten und wieder starten.

Erstellen Sie eine statische -IP-Adresse und fügen Sie diese an Ihre LAMP-Instance an. Weitere Informationen finden Sie unter Erstellen einer statischen IP und Anfügen an eine Instance in der Lightsail-Dokumentation.

1. Wählen Sie auf der Registerkarte Instances der Lightsail-Startseite Ihre laufende LAMP-Instance aus.



2. Wählen Sie auf der Registerkarte Netzwerk die Option Statische IP anfügen aus.



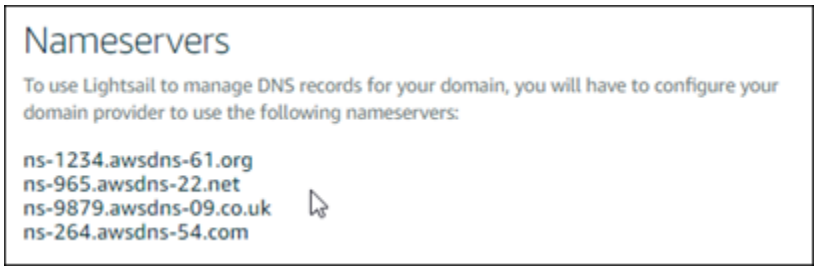
3. Geben Sie Ihrer statischen IP einen Namen und wählen Sie dann Erstellen und Anfügen aus.

Schritt 6: Erstellen einer DNS-Zone und Zuordnung Ihrer LAMP-Instance zu einer Domain

Übertragen Sie die Verwaltung der DNS-Datensätze Ihrer Domain an Lightsail. Auf diese Weise können Sie Ihrer LAMP-Instance eine Domain leichter zuordnen und alle Ressourcen Ihrer Website mithilfe der Lightsail-Konsole verwalten. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.

1. Wählen Sie auf der Registerkarte Domains und DNS der Lightsail-Startseite DNS-Zone erstellen aus.
2. Geben Sie Ihre Domain ein und wählen Sie dann Create DNS zone (DNS-Zone-erstellen).
3. Notieren Sie sich die auf der Seite aufgeführten Nameserveradressen.

   Sie fügen diese Namenserveradressen der Vergabestelle Ihres Domänennamens hinzu, um die Verwaltung der DNS-Datensätze Ihrer Domäne an Lightsail zu übertragen.

4. Nachdem die Verwaltung der DNS-Datensätze Ihrer Domain an Lightsail übertragen wurde, fügen Sie wie folgt einen A-Datensatz hinzu, der die Spitze Ihrer Domain auf Ihre LAMP-Instance verweist:

a. Wählen Sie auf der Registerkarte Zuweisungen der DNS-Zone die Option Zuweisung hinzufügen aus.

b. Wählen Sie im Feld Select a domain (Domain auswählen) die Domain oder Subdomain aus.

c. Wählen Sie in der Dropdownliste Select a resource (Ressource auswählen die LAMP-Instance aus, die Sie zuvor in diesem Tutorial erstellt haben.

d. Wählen Sie die Option Assign (Zuweisen).

Lassen Sie der Änderung Zeit, sich über das Internet-DNS zu verbreiten, bevor Ihre Domain beginnt, den Datenverkehr an Ihre LAMP-Instance weiterzuleiten.

Nächste Schritte

Hier sind einige zusätzliche Schritte, die Sie nach dem Starten einer LAMP-Instance in Amazon Lightsail ausführen können:

- Erstellen eines Snapshots Ihrer Linux-/Unix-basierten Instance
- Erstellen von zusätzlichen Blockspeicher-Datenträgern und Anfügen an Linux-basierte -Instances

Tutorial: Starten und Konfigurieren einer Windows-Server-2016-Instance

Amazon Lightsail ist der einfachste Weg, um mit Amazon Web Services (AWS) zu beginnen, wenn Sie nur virtuelle private Server benötigen. Lightsail bietet alles, was Sie benötigen, um Ihr Projekt schnell zu starten – eine virtuelle Maschine, SSD-basierten Speicher, Datenübertragung, DNS-Verwaltung und eine statische IP – zu einem niedrigen, vorhersehbaren Preis.

In diesem Tutorial erfahren Sie, wie Sie eine Windows Server 2016-Instance auf Lightsail starten und konfigurieren. Es beschreibt die Schritte, um sich über RDP mit Ihrer Instance zu verbinden, eine statische IP zu erstellen und sie an Ihre Instance anzufügen, und eine DNS-Zone zu erstellen und Ihrer Domäne zuzuordnen. Wenn Sie mit diesem Tutorial fertig sind, verfügen Sie über die Grundlagen, um Ihre Instance auf Lightsail zum Laufen zu bringen.

Inhalt

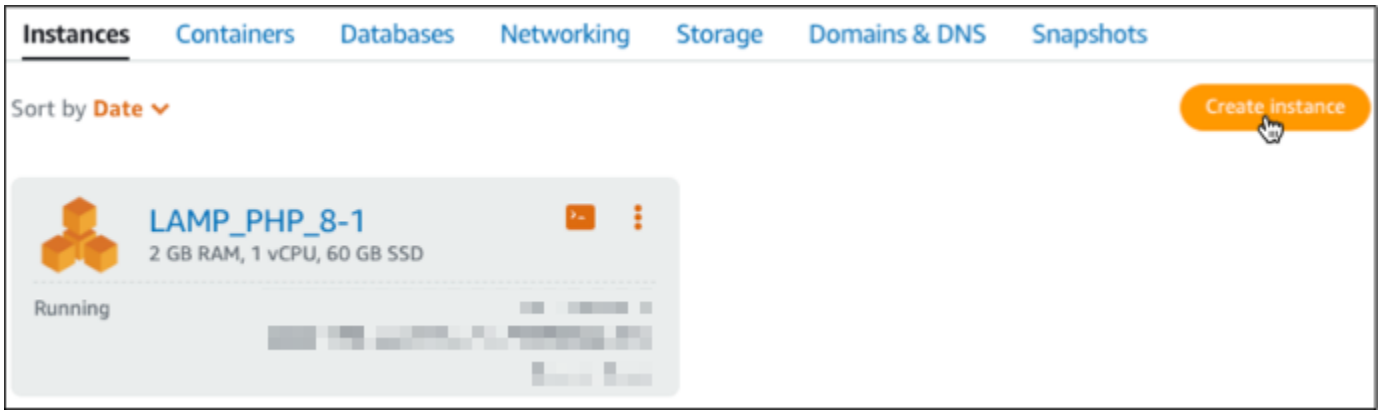
Schritt 1: Registrieren bei AWS

Für dieses Tutorial ist ein AWS-Konto erforderlich. Registrieren Sie sich bei AWS oder melden Sie sich bei AWS an, wenn Sie bereits ein Konto haben.

Schritt 2: Erstellen einer Windows Server 2016-Instance in Lightsail

Starten Sie Ihre Windows Server 2016-Instance in Lightsail. Weitere Informationen finden Sie unter Erste Schritte mit Windows-Server-basierten Instances.

1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Registerkarte Instances der Lightsail-Startseite die Option Instance erstellen aus.

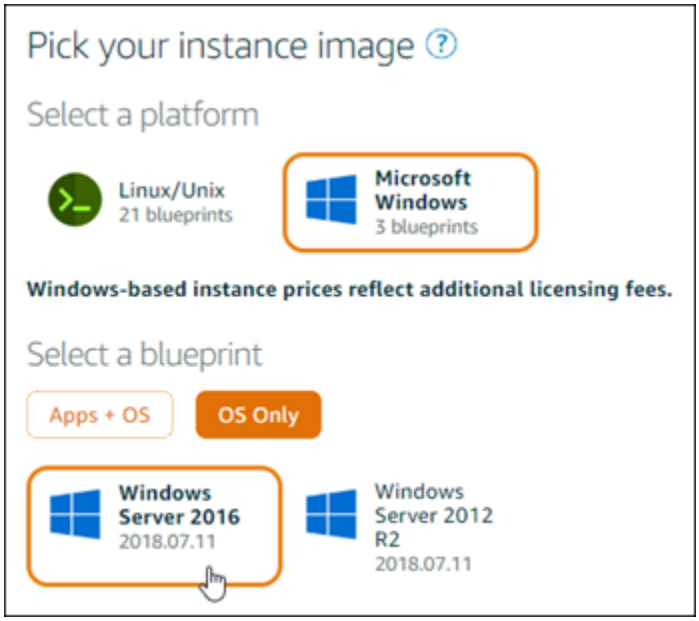


3. Wählen Sie die AWS-Region und Availability Zone für Ihre Instance.

4. Wählen Sie Ihr Instance-Image.

   a. Wählen Sie Microsoft Windows als Plattform aus.

   b. Wählen Sie OS Only (Nur Betriebssystem) und dann Windows Server 2016 als Vorlage.



5. Wählen Sie einen Instance-Plan.

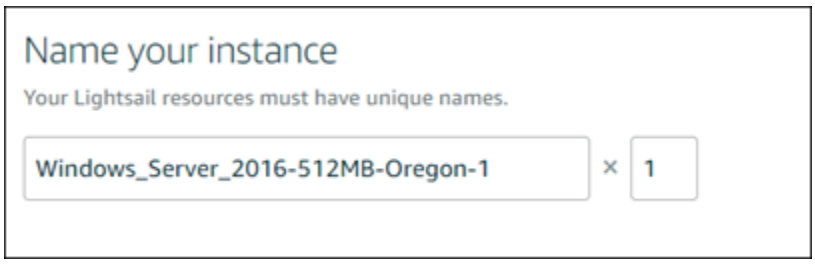
   Ein Plan beinhaltet niedrige, vorhersehbare Kosten, die Maschinenkonfiguration (RAM, SSD, vCPU) und die Zuteilung der Datenübertragung. Sie können den Lightsail-Plan im Wert von 8 USD kostenlos für einen Monat (bis zu 750 Stunden) testen. AWSrechnet Ihrem Konto einen kostenlosen Monat an.

   > **Note**
   >
   > Im Rahmen des AWS kostenlosen Kontingents für können Sie kostenlos mit Amazon Lightsail für ausgewählte Instance-Pakete beginnen. Weitere Informationen finden Sie unter AWS Kostenloses Kontingent auf der Seite Amazon Lightsail – Preise.

6. Geben Sie einen Namen für Ihre Instance ein.

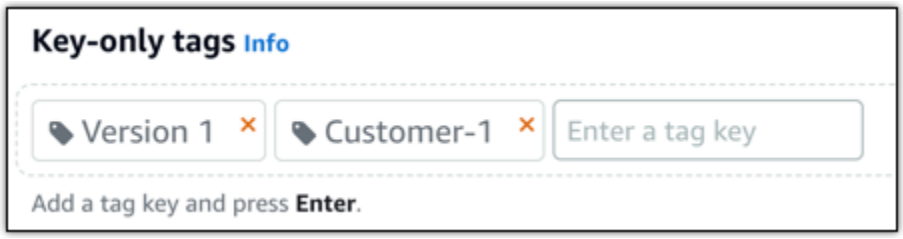
   Ressourcennamen:

   - Muss in jedem AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.



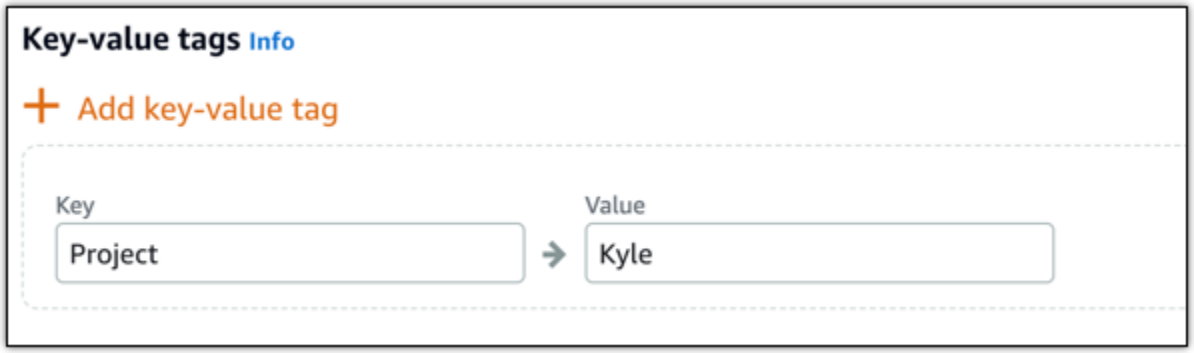
7. Wählen Sie eine der folgenden Optionen, um Ihrer Instance Tags hinzuzufügen:

   - Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.



- Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

  Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.



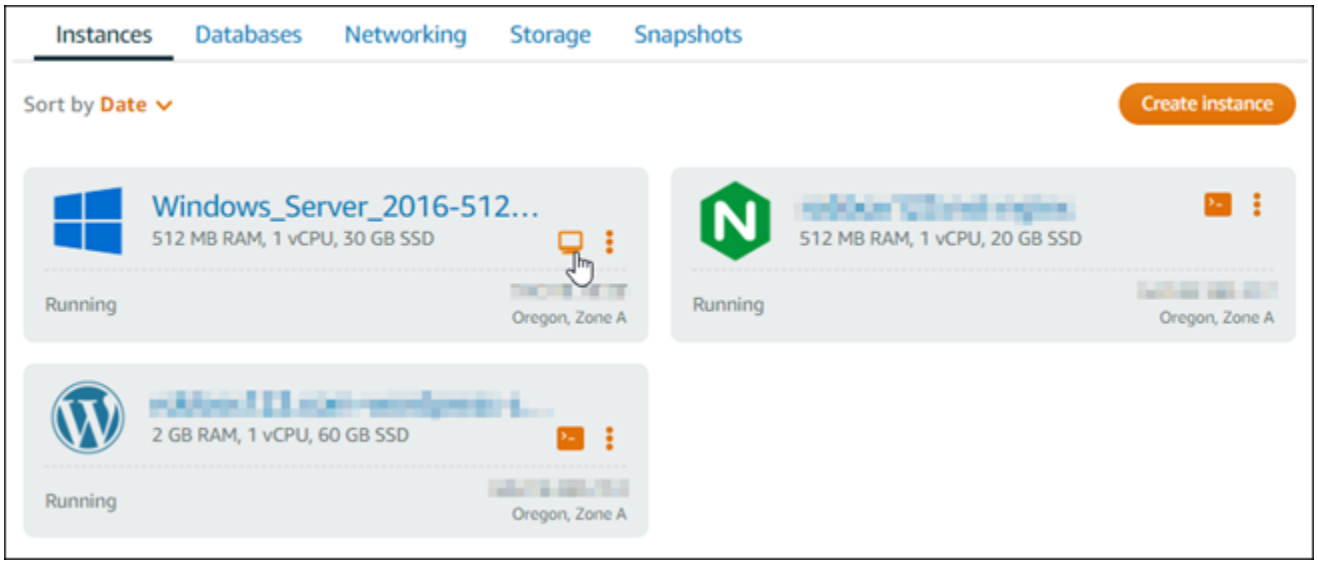
> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

8. Wählen Sie Create instance (Instance erstellen).

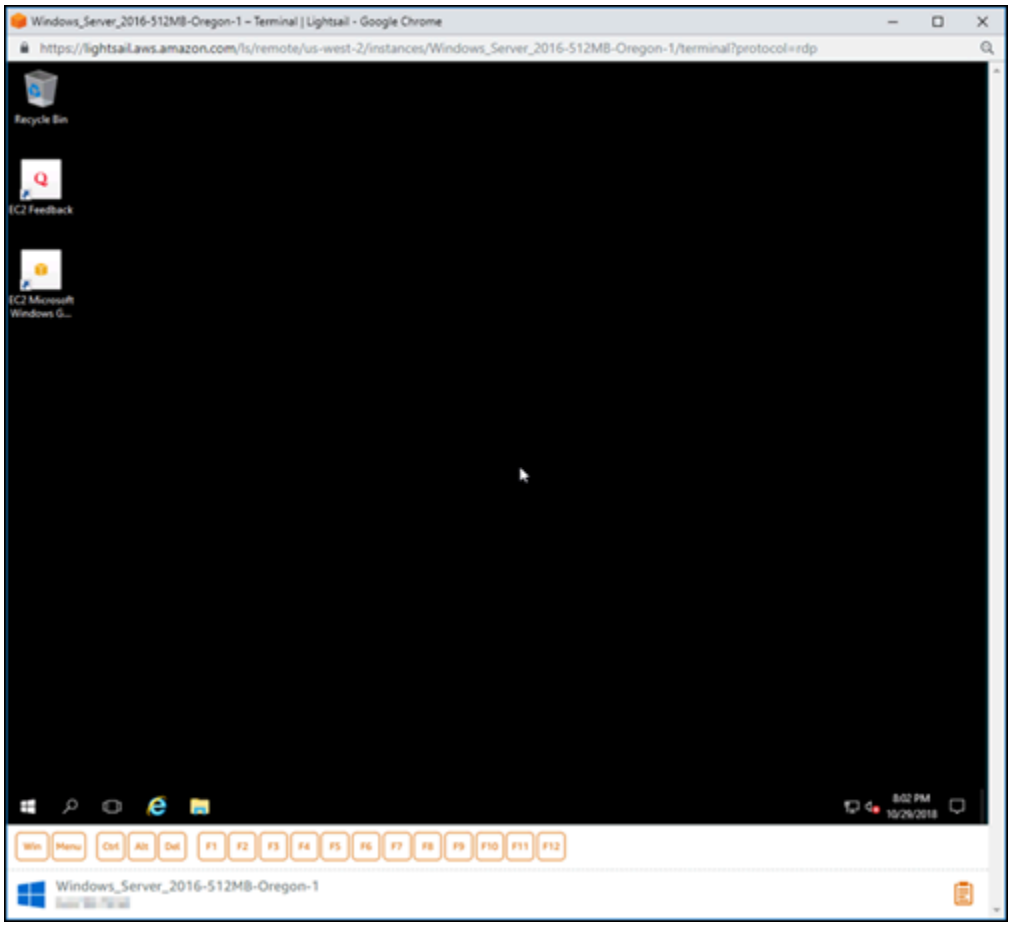
Schritt 3: Herstellen einer Verbindung zu Ihrer Windows-Server-2016-Instance über RDP

Stellen Sie über den browserbasierten RDP-Client in der Lightsail-Konsole eine Verbindung zu Ihrer Windows Server 2016-Instance her. Weitere Informationen finden Sie unter Verbinden mit Ihrer Windows-Instance.

1. Wählen Sie auf der Registerkarte Instances der Lightsail-Startseite das RDP-Schnellverbindungssymbol für Ihre Windows Server 2016-Instance aus.



2. Nachdem sich das browserbasierte RDP-Client-Fenster geöffnet hat, können Sie mit der Konfiguration Ihrer Windows Server 2016-Instance beginnen:

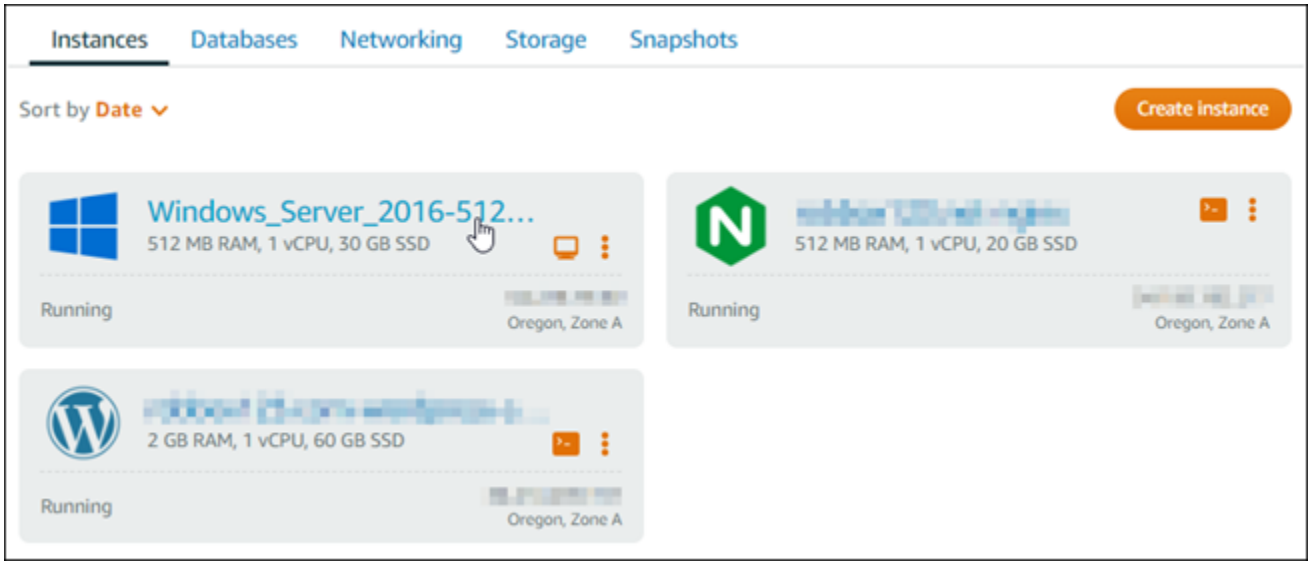


Schritt 4: Erstellen Sie eine statische IP-Adresse und fügen Sie diese an Ihre Windows-Server-2016-Instance an

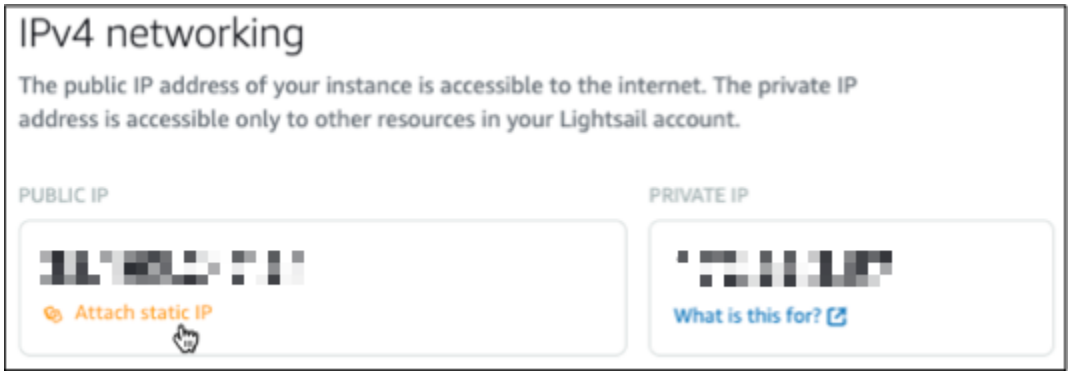
Die standardmäßige öffentliche IP für Ihre Windows Server 2016-Instance ändert sich, wenn Sie die Instance stoppen und starten. Eine statische IP-Adresse, die einer Instance zugeordnet ist, bleibt gleich, auch wenn Sie Ihre Instance anhalten und wieder starten.

Erstellen Sie eine statische -IP-Adresse und fügen Sie diese an Ihre Windows Server 2016-Instance an. Weitere Informationen finden Sie unter Erstellen einer statischen IP und Anfügen an eine Instance in der Lightsail-Dokumentation.

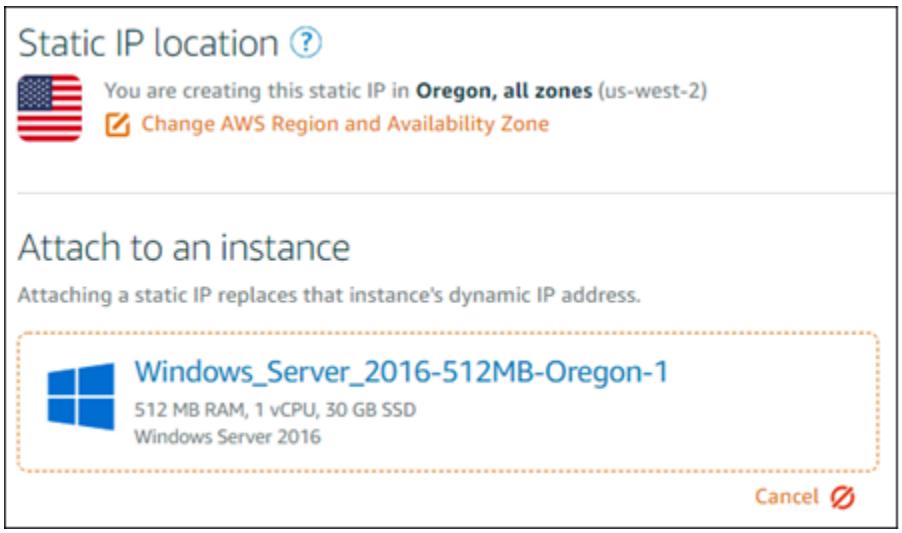
1. Wählen Sie auf der Registerkarte Instances der Lightsail-Startseite Ihre laufende Windows Server 2016-Instance aus.



2. Wählen Sie auf der Registerkarte Networking (Netzwerk) die Option Create static IP (Statische IP erstellen).



3. Der Ort der statischen IP und die angefügte Instance sind vorab ausgewählt, basierend auf die Instance, die Sie zu einem früheren Zeitpunkt in diesem Tutorial gewählt haben.



4. Geben Sie einen Namen für Ihre statische IP ein.

   Ressourcennamen:

   - Muss in jedem AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

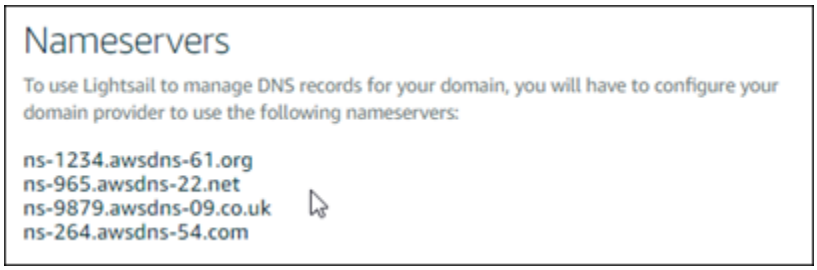
5. Wählen Sie Erstellen.

Schritt 5: Erstellen Sie eine DNS-Zone und ordnen Sie Ihrer Windows-Server-2016-Instance eine Domain zu

Übertragen Sie die Verwaltung der DNS-Datensätze Ihrer Domain an Lightsail. Auf diese Weise können Sie Ihrer Windows Server 2016-Instance eine Domain einfacher zuordnen und alle Ressourcen Ihrer Website mithilfe der Lightsail-Konsole verwalten. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain in der Lightsail-Dokumentation.

1. Wählen Sie auf der Registerkarte Domains und DNS der Lightsail-Startseite DNS-Zone erstellen aus.
2. Geben Sie Ihre Domain ein und wählen Sie dann Create DNS zone (DNS-Zone-erstellen).
3. Notieren Sie sich die auf der Seite aufgeführten Nameserveradressen.

   Sie fügen diese Namenserveradressen der Vergabestelle Ihres Domänennamens hinzu, um die Verwaltung der DNS-Datensätze Ihrer Domäne an Lightsail zu übertragen.

4. Nachdem die Verwaltung der DNS-Datensätze Ihrer Domain an Lightsail übertragen wurde, fügen Sie wie folgt einen A-Datensatz hinzu, der die Spitze Ihrer Domain auf Ihre LAMP-Instance verweist:

   a. Wählen Sie auf der Registerkarte Zuweisungen der DNS-Zone die Option Zuweisung hinzufügen aus.

   b. Wählen Sie im Feld Select a domain (Domain auswählen) die Domain oder Subdomain aus.

   c. Wählen Sie in der Dropdownliste Select a resource (Ressource auswählen die LAMP-Instance aus, die Sie zuvor in diesem Tutorial erstellt haben.

   d. Wählen Sie die Option Assign (Zuweisen).

   Lassen Sie der Änderung Zeit, sich über das Internet-DNS zu verbreiten, bevor Ihre Domain beginnt, den Datenverkehr an Ihre LAMP-Instance weiterzuleiten.

Nächste Schritte

Hier sind einige zusätzliche Schritte, die Sie nach dem Starten einer Windows Server 2016-Instance in Amazon Lightsail ausführen können:

- Erstellen eines Snapshots Ihrer Windows-Server-Instance
- Bewährte Methoden zum Sichern von Windows Server-basierten Lightsail-Instances
- Erstellen eines Blockspeicher-Datenträgers zum Verbinden mit Ihrer Windows-Server-Instance
- Erweitern des Speicherplatzes Ihrer Windows-Server-Instance

Weitere Informationen zu Amazon Lightsail

Die folgende Liste enthält Links zu zusätzlichen Informationen für Amazon Lightsail, die nicht im Lightsail-Benutzerhandbuch enthalten sind.

Inhalt

Blogs

- Überwachen des Zustands von Amazon Lightsail-Instances mit Datadog

  30. März 2022 – Erfahren Sie, wie das Überwachen von Lightsail-Workloads mit Datadog Ihnen dabei helfen kann, die Anwendungsleistung sicherzustellen und die Kosten zu kontrollieren.
- Wie Sie Galaxy für die Forschung in AWS unter Verwendung vonAmazon Lightsail einrichten

  13. Januar 2022 – Stellen Sie Galaxy, einen wissenschaftlichen Workflow, Datenintegration und digitale Aufbewahrungsplattform in Lightsail bereit.
- Was passiert, wenn Sie eine URL in Ihren Browser eingeben

  26. August 2021 – Was passiert, wenn Sie eine URL in Ihren Browser eingeben und die Eingabetaste drücken?
- Überwachen der Speicherauslastung in einer Amazon Lightsail-Instance

14. Juni 2021 – Konfigurieren Sie eine Lightsail-Instance zum Senden der Speicherauslastung an Amazon CloudWatch für Überwachung, Alarmierung und Benachrichtigungen.

- Reibungsloses Hosten von containerisierten ASP.NET-Web-Apps mit Amazon Lightsail

10. Juni 2021 – So verwenden Sie eine containerisierte ASP.NET-Webanwendung, die sich mit einer PostgreSQL-Datenbank verbindet, und stellen sie in Lightsail bereit.

- Starten einer WordPress-Website mit Amazon Lightsail-Containern

05. April 2021 Lightsail – Starten Sie eine WordPress-Website mit -Containern und einer Lightsail-Datenbank.

- Lightsail-Container: Eine einfache Möglichkeit, Ihre Container in der Cloud zu betreiben

13. November 2020 – Stellen Sie Ihre containerbasierten Workloads in Lightsail bereit.

- Migrieren von Webservices von Amazon Lightsail zu Amazon EC2

16. Oktober 2020 – Richten Sie eine Produktionsumgebung in Amazon EC2 ein und migrieren Sie einen Webservice in diese Umgebung von Lightsail aus.

- Aufbauen eines Graylog-Servers für die Ausführung auf einer Amazon Lightsail-Instance

28. Juli 2020 – So bauen Sie einen Graylog-Server in Lightsail auf.

- Verbesserung der Website-Leistung mit einem Lightsail-Netzwerk zur Bereitstellung von Inhalten

23. Juli 2020 – Konfigurieren Sie eine Lightsail-Verteilung so, dass sie sowohl mit einem Standard-Webserver als auch mit WordPress funktioniert..

- Proaktives Überwachen der Systemleistung auf Amazon Lightsail-Instances

4. Juni 2020 – Konfigurieren Sie eine Warnung über Burstable Capacity, damit Sie Probleme mit der Systemleistung verhindern können, bevor sie sich auf Ihre Benutzer auswirken.

- Verbessern der Standortsicherheit mit neuen Lightsail-Firewall-Funktionen

7. Mai 2020 – Beschränken Sie den Remotezugriff mit SSH auf eine einzige Quell-IP-Adresse.

- Verwenden von CodeDeploy und CodePipeline zum Bereitstellen von Anwendungen für Amazon Lightsail

23. April 2020 – Konfigurieren Sie Lightsail, um mit CodeDeploy und CodePipeline zu arbeiten, um eine Anwendung jedes Mal automatisch bereitzustellen (oder zu aktualisieren), wenn Sie eine Änderung an GitHub übertragen.

- Verwenden von Load Balancers in Amazon Lightsail

  21. April 2020 – Wie Sie eine einfache Node.js-Webanwendung mit Hilfe eines Amazon Lightsail-Load Balancers ausbalancieren.

- Erstellen eines Fototagebuchs in Amazon Lightsail mit Ghost

  23. März 2020 – Starten Sie ein Fototagebuch mit Ghost in Lightsail.

- Tipps und Tricks für die Amazon Lightsail-Datenbank

  23. März 2020 – Nutzen Sie die erweiterten Features von Amazon Relational Database Service (Amazon RDS).

- Konfigurieren und Verwenden von Überwachung und Benachrichtigungen

  27. Februar 2020 – Erstellen von Benachrichtigungskontakten, Erstellen eines neuen Alarms und Testen von Benachrichtigungen mit Ressourcenüberwachung.

- Bereitstellen einer hochverfügbaren WordPress-Site in Amazon Lightsail, Teil 1: Implementieren einer hochverfügbaren Lightsail-Datenbank mit WordPress

  22. Oktober 2019 – Erstellen einer hochverfügbaren WordPress-Site in Lightsail, Teil 1.

- Bereitstellen einer hochverfügbaren WordPress-Site in Amazon Lightsail, Teil 2: Verwenden von Amazon S3 mit WordPress zur sicheren Bereitstellung von Mediendateien

  31. Oktober 2019 – Erstellen einer hochverfügbaren WordPress-Site in Lightsail, Teil 2.

- Bereitstellen einer hochverfügbaren WordPress-Site in Amazon Lightsail, Teil 3: Erhöhen der Sicherheit und Leistung mit Amazon CloudFront

  7. November 2019 – Erstellen einer hochverfügbaren WordPress-Site in Lightsail, Teil 3.

- Bereitstellen einer hochverfügbaren WordPress-Site in Amazon Lightsail, Teil 4: Steigern der Leistung und Skalierbarkeit mit einem Lightsail-Load Balancer

  14. November 2019 – Erstellen einer hochverfügbaren WordPress-Site in Lightsail, Teil 4.

- Aufbau einer Pocket-Plattform als Service mit Amazon Lightsail

  8. Oktober 2019 – Zusammenstellen einer Pocket-Plattform in Lightsail.

- Bereitstellen eines Nginx-basierten HTTP/HTTPS-Load Balancers mit Amazon Lightsail

  8. Juli 2019 – Einrichten eines NGINX-basierten Load Balancers innerhalb einer Lightsail-Instance.

- Neu in der AWS Cloud? Amazon Lightsail kann helfen

27. März 2019 – Erste Schritte mit Amazon Lightsail.

- Neu – Verwaltete Datenbanken für Amazon Lightsail

16. Oktober 2018 – Erstellen Sie mit ein paar Klicks eine verwaltete Datenbank.

- Amazon Lightsail-Update: Mehr Instance-Größen und Preissenkungen

23. August 2018 – Übersicht über die Lightsail-Instance.

- Amazon Lightsail: Die Leistungsfähigkeit von AWS, die Einfachheit eines VPS

30. November 2016 – Startankündigung von Lightsail.

Tutorials

Top 5 der Praxis-Tutorials:

1. Erstellen einer lastenverteilten WordPress-Website

   8. September 2021 – Starten Sie eine hochverfügbare WordPress-Website mit Lightsail.

2. Migrieren und Verwalten einer WordPress-Website mit Amazon Lightsail

   22. Februar 2021 – Starten Sie einen Klon Ihrer WordPress-Website in Lightsail mit der Seahorse-Software.

3. Starten einer virtuellen Linux-Maschine

   11. September 2020 – Starten, konfigurieren und verbinden Sie sich mit einer Linux-Instance mit Lightsail.

4. Starten einer virtuellen Windows-Maschine

   11. September 2020 – Starten, konfigurieren und verbinden Sie sich mit einer Windows-Instance mit Lightsail.

5. Starten eine cPanel- und WHM-Instance in Amazon Lightsail

   27. Juli 2020 – In diesem Tutorial finden Sie einige erste Schritte, die Sie unternehmen können, nachdem Ihre cPanel- und WHM-Instance in Lightsail eingerichtet wurde und ausgeführt wird.

- Einrichten und Konfigurieren von Magento in Amazon Lightsail

11. August 2021 – Richten Sie eine ECommerce-Website ein und führen Sie sie aus.

- So verbinden Sie Ihre WordPress-Site mit einem Objektspeicher-Bucket

14. Juli 2021 – Richten Sie Ihre WordPress-Website in Lightsail ein und verbinden Sie die Website mit einem Lightsail-Bucket.

- Erstellen von Objektspeicher-Buckets

14. Juli 2021 – Erstellen Sie einen Objektspeicher-Bucket in Amazon Lightsail.

- Verbinden einer WordPress-Website mit einem Amazon Lightsail-Bucket und einer Verteilung

14. Juli 2021 – Konfigurieren Sie Ihren Lightsail-Bucket als Ursprung einer Content Delivery Network (CDN)-Verteilung von Lightsail.

- Einrichten und Konfigurieren von Plesk

22. April 2021 – Richten Sie einen Plesk-Hosting-Stack in Lightsail ein und führen Sie ihn aus.

- So richten Sie eine ECommerce-Website von Prestashop ein

01. April 2021 – Starten und konfigurieren Sie eine Lightsail-Instance, die die Vorlage von PrestaShop Certified by Bitnami verwendet.

- So verwenden Sie Amazon EFS mit Amazon Lightsail

15. März 2021 – Erstellen Sie ein Amazon-EFS-Dateisystem von Lightsail-Instances mit VPC-Peering ein und stellen Sie eine Verbindung damit her.

- So richten Sie einen Nginx-Reverse-Proxy ein

10. Februar 2021 – Richten Sie einen Nginx-Reverse-Proxy mit Lightsail-Containern ein.

- So stellen Sie eine Flask-App bereit

3. Februar 2021 – Erfahren Sie, wie Sie eine Flask-Anwendung mit Lightsail-Containern bereitstellen.

- Erstellen, Verteilen und Bereitstellen von Container-Images mit Amazon Lightsail

11. November 2020 – Erstellen Sie mit einer Docker-Datei ein Container-Image auf Ihrem lokalen Computer.

- Erstellen einer Drupal-Website

11. September 2020 – Stellen Sie eine produktionsbereite Drupal-Website in Lightsail bereit und hosten Sie sie.

- Erstellen einer LAMP-Stack-Web-App

9. September 2020 – Starten und führen Sie eine hochverfügbare PHP-Webanwendung in Lightsail aus.

- Konfiguration Ihrer WordPress-Instance für die Zusammenarbeit mit Ihrer Verteilung

16. Juli 2020 – Konfigurieren Sie Ihre WordPress-Instance für die Zusammenarbeit mit Ihrer Lightsail-Verteilung.

- Starten einer WordPress-Website

23. März 2020 – Richten Sie eine Website mit WordPress ein, das auf einer virtuellen Lightsail-Maschine installiert ist.

- Hosten einer .NET-Anwendung

20. März 2020 – Erstellen Sie eine .NET-Anwendung mit Lightsail und stellen Sie sie bereit.

- Ordnen Sie Ihre Domain auf Amazon Route 53 Ihren Lightsail-Ressourcen zu

Leiten Sie den Datenverkehr für Ihre Domäne, z. B. example.com, zu Ihren Lightsail-Ressourcen um.

Videos

- Amazon Lightsail-Tutorial: Bereitstellen einer Django-App

14. Juli 2021 – In diesem Tutorial erstellen Sie eine Django-Anwendung.

- Amazon Lightsail-Tutorial: Bereitstellen einer Flask-App

14. Juli 2021 – In diesem Tutorial erstellen Sie eine Flask-Anwendung.

- Amazon Lightsail-Tutorial: Bereitstellen eines NGINX-Reverse-Proxy

14. Juli 2021 – Erstellen einer Flask-Anwendung, Erstellen eines Docker-Containers, Erstellen eines Container-Service in Lightsail und Bereitstellen der Anwendung.

- Amazon Lightsail-Tutorial: Bereitstellen einer E-Commerce-Site

14. Juli 2021 – Starten und konfigurieren Sie eine Lightsail-Instance, die die Vorlage von PrestaShop Certified by Bitnami verwendet.

- Bereitstellen einer containerisierten Anwendung in Amazon Lightsail

29. Dezember 2020 – Erfahren Sie, wie Sie eine containerisierte Anwendung in Lightsail bereitstellen.

- Amazon Lightsail-Tutorial: Erstellen einer Drupal-Website

31. August 2020 – Starten und konfigurieren Sie eine Drupal-Instance.

- Amazon Lightsail-Tutorial: Bereitstellen einer LAMP Stack-App

31. August 2020 – Stellen Sie eine LAMP (Linux Apache MySQL PHP)-Stack-Anwendung auf einer einzigen Lightsail-Instance bereit.

- Amazon Lightsail-Tutorial: Starten einer Linux-Instance

31. August 2020 – Erfahren Sie, wie Sie eine Linux-Instance starten.

- Amazon Lightsail-Tutorial: Starten einer Windows-Instance

31. August 2020 – Erfahren Sie, wie Sie eine Windows-Instance starten.

- Amazon Lightsail-Tutorial: Betreiben Ihres eigenen Minecraft-Servers

31. August 2020 – Erfahren Sie, wie Sie einen dedizierten Minecraft-Server einrichten.

- Einführung in Amazon Lightsail-Tutorials

31. August 2020 – Beginnen Sie noch heute Ihren Weg in die Cloud mit Lightsail.

- Amazon Lightsail: Die einfachste Möglichkeit, um in AWS zu beginnen

20. März 2020 – Lightsail ist die einfachste Möglichkeit, um in AWS zu beginnen. Es bietet virtuelle Server, Speicher, Datenbanken und Netzwerke und einen kostengünstigen Monatstarif.

- Konfigurieren einer Plesk-Instance in Amazon Lightsail

27. März 2019 – Erfahren Sie, wie Sie eine Plesk-Instance in Lightsail konfigurieren.

- Konfigurieren von WordPress Multisite in Amazon Lightsail

15. Januar 2019 – Erfahren Sie, wie Sie eine WordPress-Multisite-Instance in Lightsail konfigurieren.

- Verwaltung von Lightsail

9. Oktober 2018 – Werfen Sie einen kurzen Blick auf Lightsail-Schlüssel-Feature.

- Bereitstellen einer MEAN Stack-App in Amazon Lightsail

  5. Juni 2018 – Verwenden Sie die MEAN-Vorlage von Lightsail zur Bereitstellung einer benutzerdefinierten Anwendung in der Cloud.

- Bereitstellen einer WordPress-Instance in Amazon Lightsail

  5. Juni 2018 – Stellen Sie eine WordPress-Instance in Lightsail bereit.

Tutorial: Migrieren von Daten aus einer MySQL-5.6-Datenbank in eine neuere Datenbankversion

In diesem Tutorial zeigen wir Ihnen, wie Sie Daten aus einer MySQL-5.6-Datenbank in eine neue MySQL-5.7-Datenbank in Amazon Lightsail migrieren. Um die Migration durchzuführen, stellen Sie eine Verbindung zu Ihrer MySQL-5.6-Datenbank her und exportieren die vorhandenen Daten. Anschließend stellen Sie eine Verbindung zur MySQL-5.7-Datenbank her und importieren die Daten. Nachdem die neue Datenbank über die erforderlichen Daten verfügt, können Sie die Anwendung neu konfigurieren, um eine Verbindung mit der neuen Datenbank herzustellen.

Inhalt

Schritt 1: Verstehen der Änderungen

Der Übergang von einer MySQL-5.6-Datenbank zu einer MySQL-5.7-Datenbank wird als ein Upgrade der Hauptversion angesehen. Hauptversions-Upgrades können Datenbankänderungen enthalten, die nicht mit vorhandenen Anwendungen rückwärts kompatibel sind. Sie sollten jedes Upgrade gründlich testen, bevor Sie es auf Ihre Produktions-Instances anwenden. Weitere Informationen finden Sie unter Änderungen in MySQL-5.7 in den MySQL-Unterlagen.

Wir empfehlen, dass Sie Ihre Daten zunächst aus Ihrer bestehenden MySQL-5.6-Datenbank in eine neue MySQL-5.7-Datenbank migrieren. Testen Sie dann Ihre Anwendung mit Ihrer neuen MySQL-5.7-Datenbank auf einer Vorproduktion-Instance. Wenn sich Ihre Anwendung wie erwartet verhält, wenden Sie die Änderung auf Ihre Anwendung in der Produktion-Instance an. Um einen Schritt weiter zu gehen, können Sie dann Ihre Daten aus Ihrer bestehenden MySQL-5.7-Datenbank in eine neue MySQL-8.0-Datenbank migrieren, Ihre Anwendung in der Vorproduktion erneut testen und die Änderung auf Ihre Anwendung in der Produktion anwenden.

Schritt 2: Erfüllen der Voraussetzungen

Sie müssen die folgenden Voraussetzungen erfüllen, bevor Sie mit den nächsten Abschnitten dieses Tutorials fortfahren:

- Installieren Sie MySQL-Workbench auf Ihrem lokalen Computer, mit dem Sie eine Verbindung zu Ihren Datenbanken herstellen, um Daten zu exportieren und zu importieren. Weitere Informationen finden Sie unter MySQL-Workbench herunterladen auf der MySQL-Website.
- Erstellen Sie eine MySQL-5.7-Datenbank in Lightsail. Weitere Informationen finden Sie unter Erstellen einer Datenbank in Amazon Lightsail.
- Aktivieren Sie den öffentlichen Modus für Ihre Datenbanken. Auf diese Weise können Sie eine Verbindung zu ihnen über MySQL-Workbench herstellen. Wenn Sie mit dem Exportieren und Importieren von Daten fertig sind, können Sie den öffentlichen Modus für Ihre Datenbanken deaktivieren. Weitere Informationen finden Sie unter Konfigurieren des öffentlichen Modus für Ihre Datenbank.
- So konfigurieren Sie MySQL-Workbench für die Verbindung zu Ihren Datenbanken. Weitere Informationen finden Sie unter Verbindung zu Ihrer MySQL-Datenbank.

Schritt 3: Verbinden Sie sich mit Ihrer MySQL-5.6-Datenbank und exportieren Sie die Daten

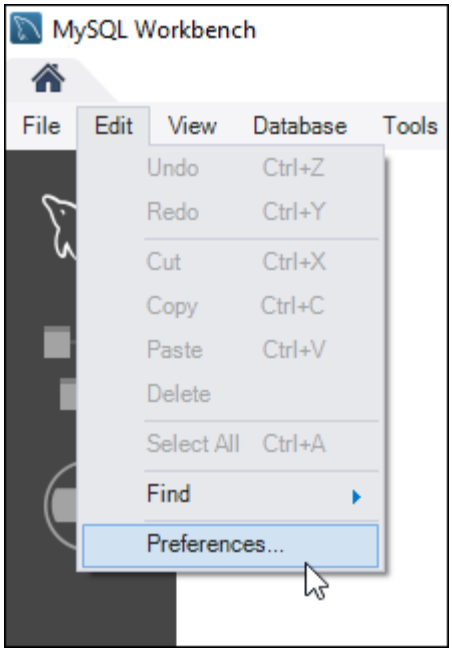
In diesem Abschnitt des Tutorials stellen Sie eine Verbindung zu Ihrer MySQL-5.6-Datenbank her und exportieren Daten aus dieser Datenbank mit MySQL-Workbench. Weitere Informationen über die Verwendung von MySQL-Workbench zum Exportieren von Daten finden Sie unter Assistent für SQL-Datenexport und -Import im MySQL-Workbench-Handbuch.

1. Stellen Sie mit MySQL-Workbench eine Verbindung zu Ihrer MySQL-5.6-Datenbank her.

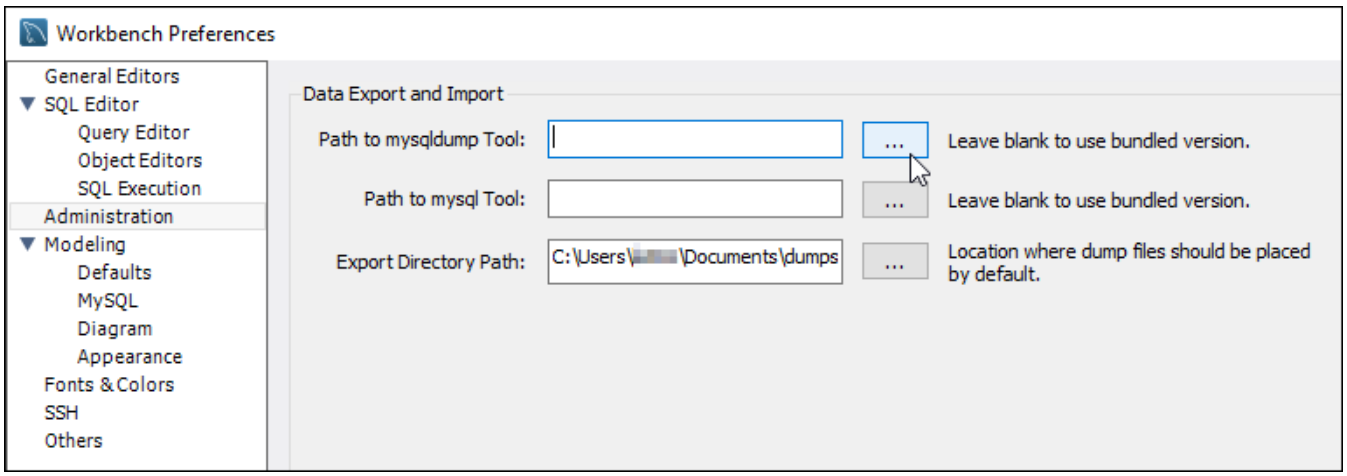
MySQL-Workbench verwendet mysqldump, um Daten zu exportieren. Die von MySQL-Workbench verwendete Version von mysqldump muss dieselbe (oder höher) wie die Version der MySQL-Datenbank sein, aus der Daten exportiert werden sollen. Wenn Sie beispielsweise Daten aus einer MySQL-5.6.51-Datenbank exportieren, müssen Sie mysqldump Version 5.6.51 oder höher verwenden. Möglicherweise müssen Sie die entsprechende Version des MySQL-Servers auf Ihrem lokalen Computer herunterladen und installieren, um sicherzustellen, dass Sie die korrekte Version von mysqldump verwenden. Informationen zum Herunterladen einer bestimmten Version des MySQL-Servers finden Sie unterMySQL Community Downloads auf der MySQL-Website. Das MySQL-Installationsprogramm für Windows MSIbietet die Möglichkeit, eine beliebige Version des MySQL-Servers herunterzuladen.

Führen Sie die folgenden Schritte aus, um die richtige Version von mysqldump auszuwählen, die in MySQL-Workbench verwendet werden soll:

1. Wählen Sie in MySQL-Workbench Bearbeiten und anschließend Präferenzen aus.

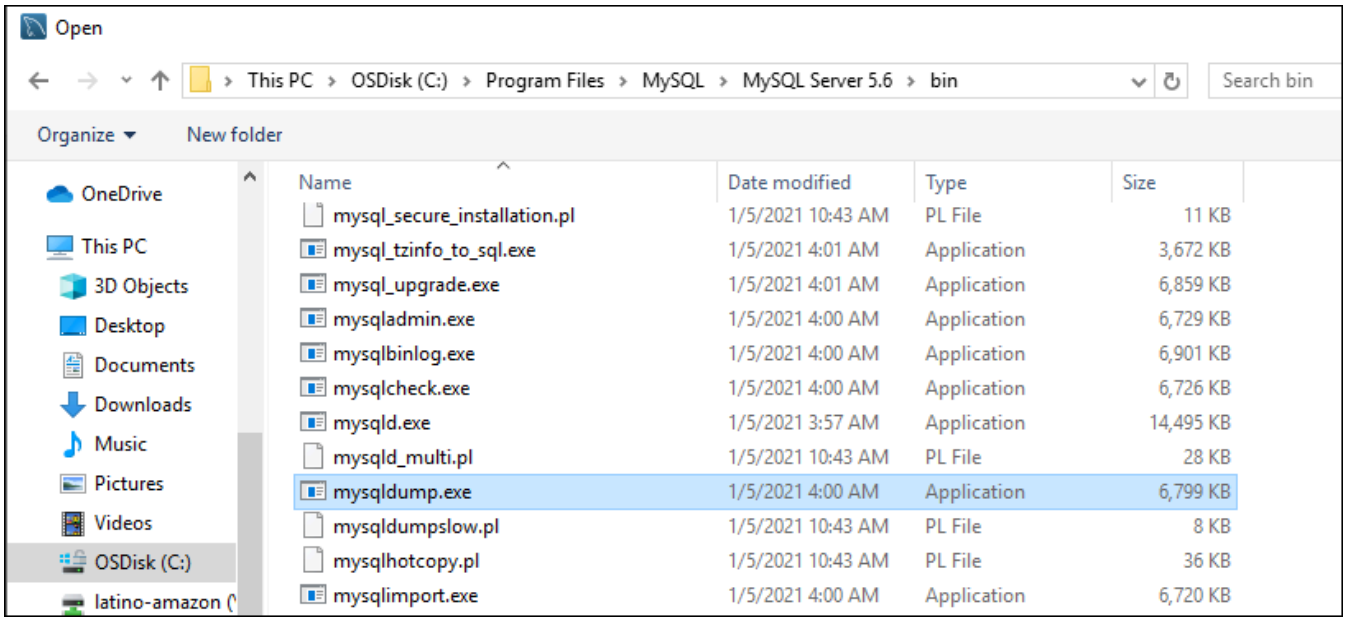


2. Wählen Sie Administration im Navigationsbereich.
3. Im FensterWorkbench-Voreinstellungen, das angezeigt wird, wählen Sie die Ellipsis-Schaltfläche neben dem Textfeld Pfad zum mysqldump-Tool.

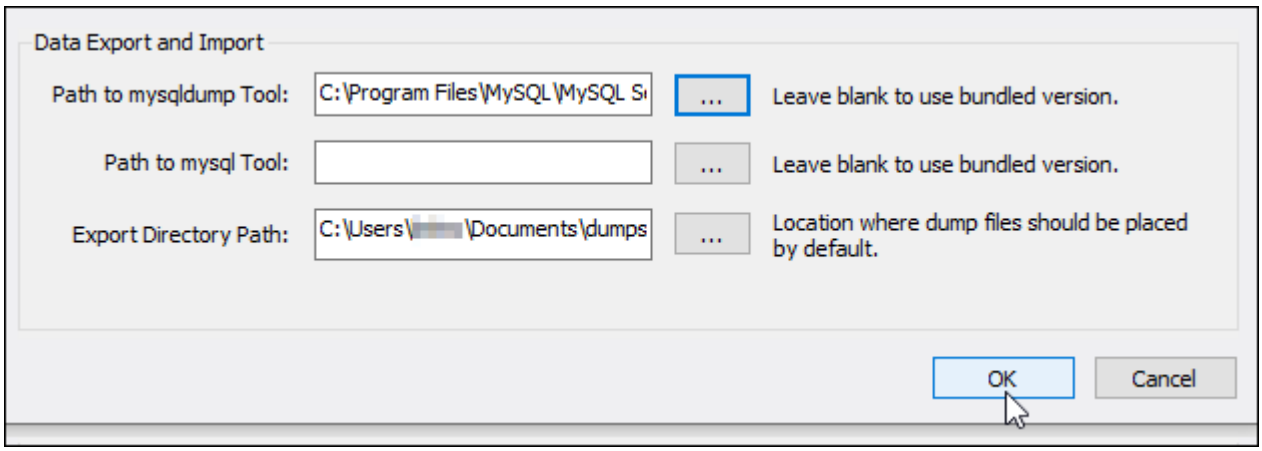


4. Navigieren Sie zum Speicherort der entsprechenden `mysqldump` ausführbaren Datei und doppelklicken Sie darauf.

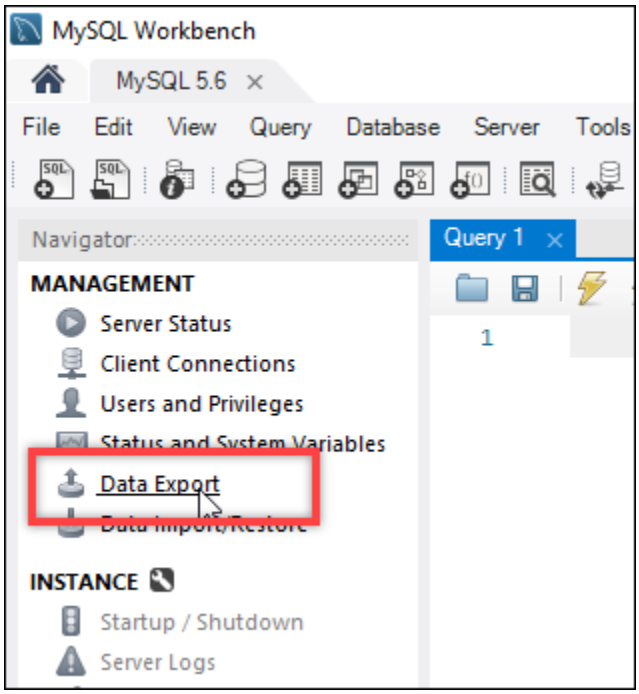
   In Windows befindet sich die `mysqldump.exe`-Datei in der Regel im `C:\Program Files \MySQL\MySQL Server 5.6\bin`-Verzeichnis. Geben Sie in Linux `which mysqldump` im Terminal ein, um zu sehen, wo sich diemysqldump-Dateil befindet.



5. Wählen Sie OK im Fenster Workbench-Voreinstellungen aus.

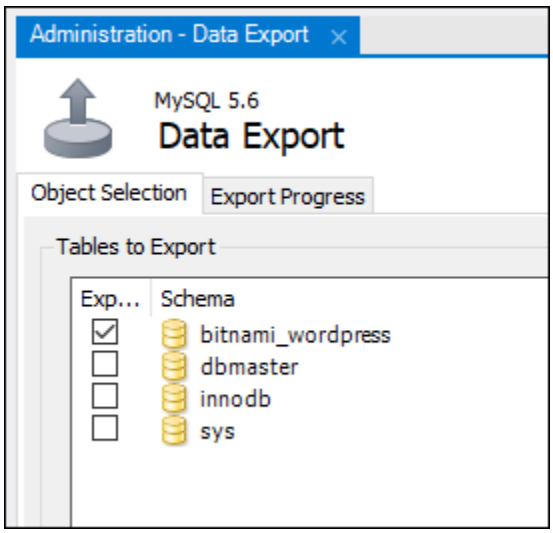


2. Wählen Sie Datenexport im Navigationsbereich aus

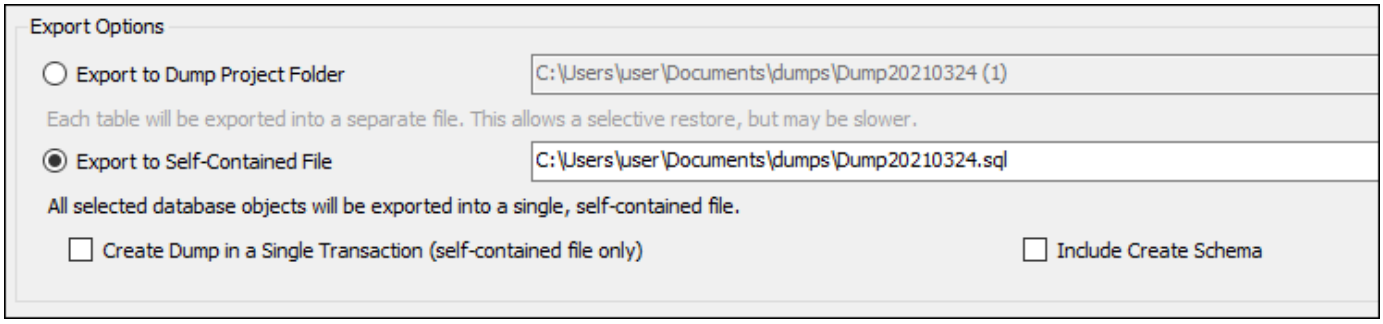


3. In der angezeigten Registerkarte Datenexport setzen Sie Häkchen neben den Tabellen, die Sie exportieren möchten.

> **Note**
>
> In diesem Beispiel haben wir die`bitnami_wordpress`-Tabelle ausgewählt, die Daten für eine WordPress-Website auf einer „Certified by Bitnami“ WordPress-Instance enthält.

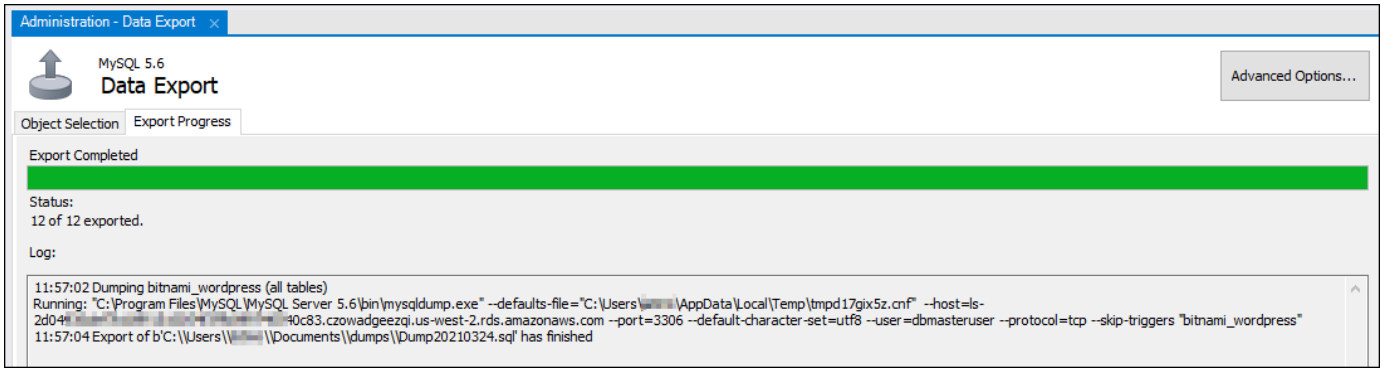


4. Im Abschnitt Exportoptionen Wählen Sie Exportieren in eigenständige Datei, und notieren Sie sich das Verzeichnis, in dem die Exportdatei gespeichert wird.



5. Wählen Sie Import starten.

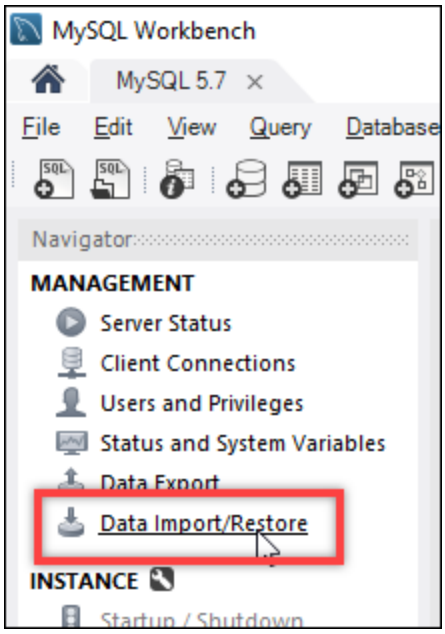
6. Warten Sie, bis der Export abgeschlossen ist, bevor Sie mit dem nächsten Abschnitt dieses Tutorials fortfahren.



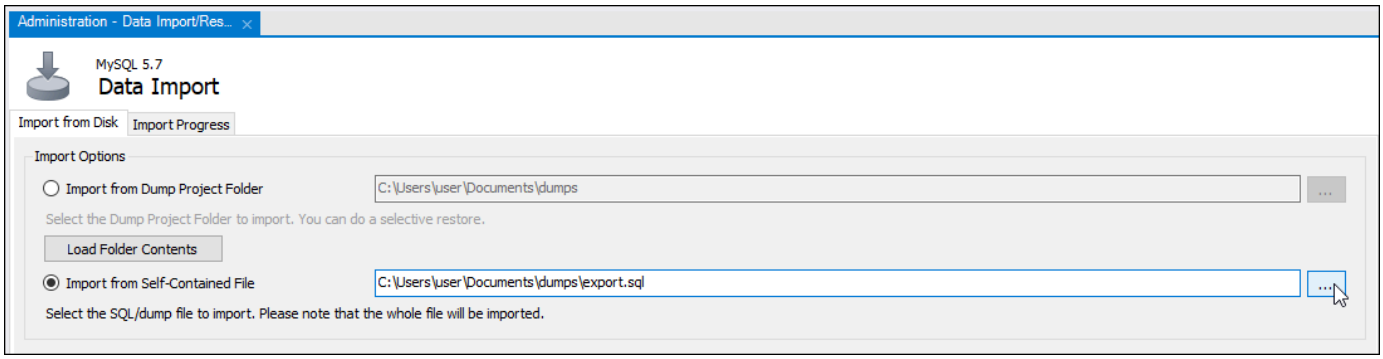
Schritt 4: Verbinden Sie sich mit Ihrer MySQL-5.7-Datenbank und importieren Sie die Daten

In diesem Abschnitt des Tutorials stellen Sie eine Verbindung zu Ihrer MySQL-5.7-Datenbank her und importieren Daten aus dieser Datenbank mit MySQL-Workbench.

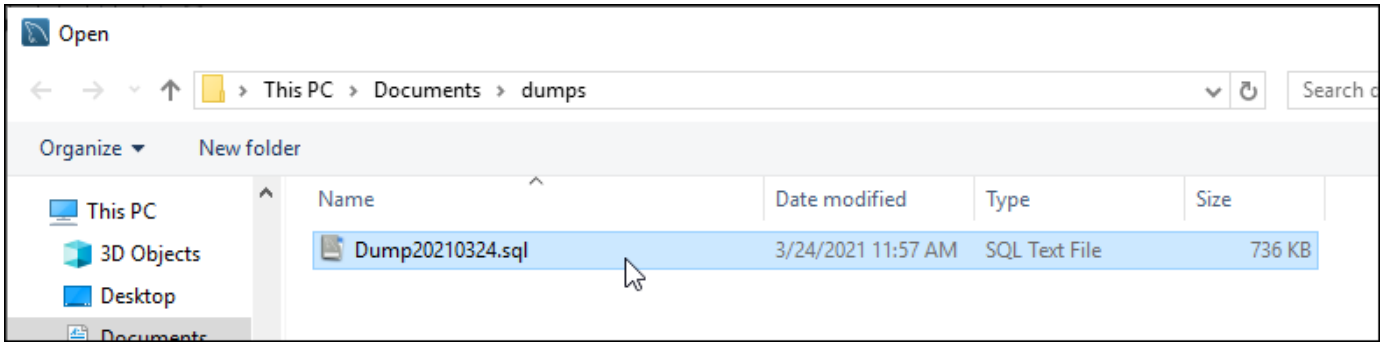
1. Stellen Sie mit MySQL-Workbench eine Verbindung zu Ihrer MySQL-5.7-Datenbank auf Ihrem lokalen Computer her.
2. Wählen Sie Datenimport/-Wiederherstellung im Navigationsbereich.



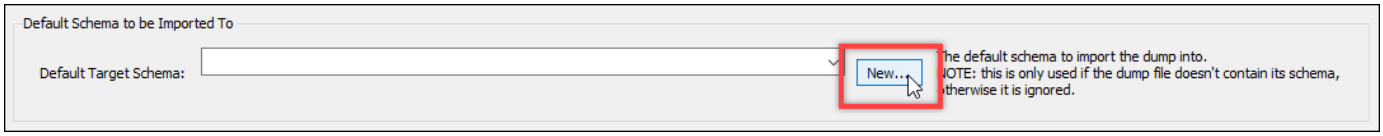
3. In der angezeigten Registerkarte Datenimport, wählen Sie Importieren aus eigenständiger Datei und wählen Sie dann die Ellipsen-Schaltfläche neben dem Textfeld aus.



4. Navigieren Sie zum Speicherort der Exportdatei, und doppelklicken Sie darauf.

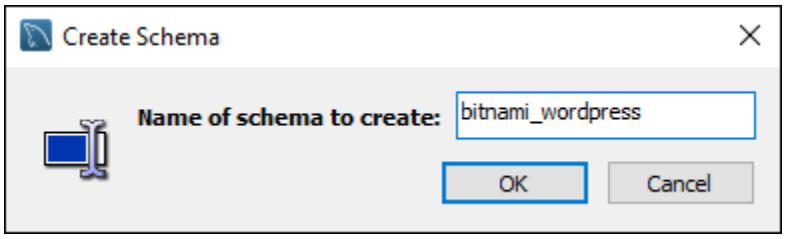


5. Wählen Sie Neu im Abschnitt Standardschema, in das importiert werden soll .

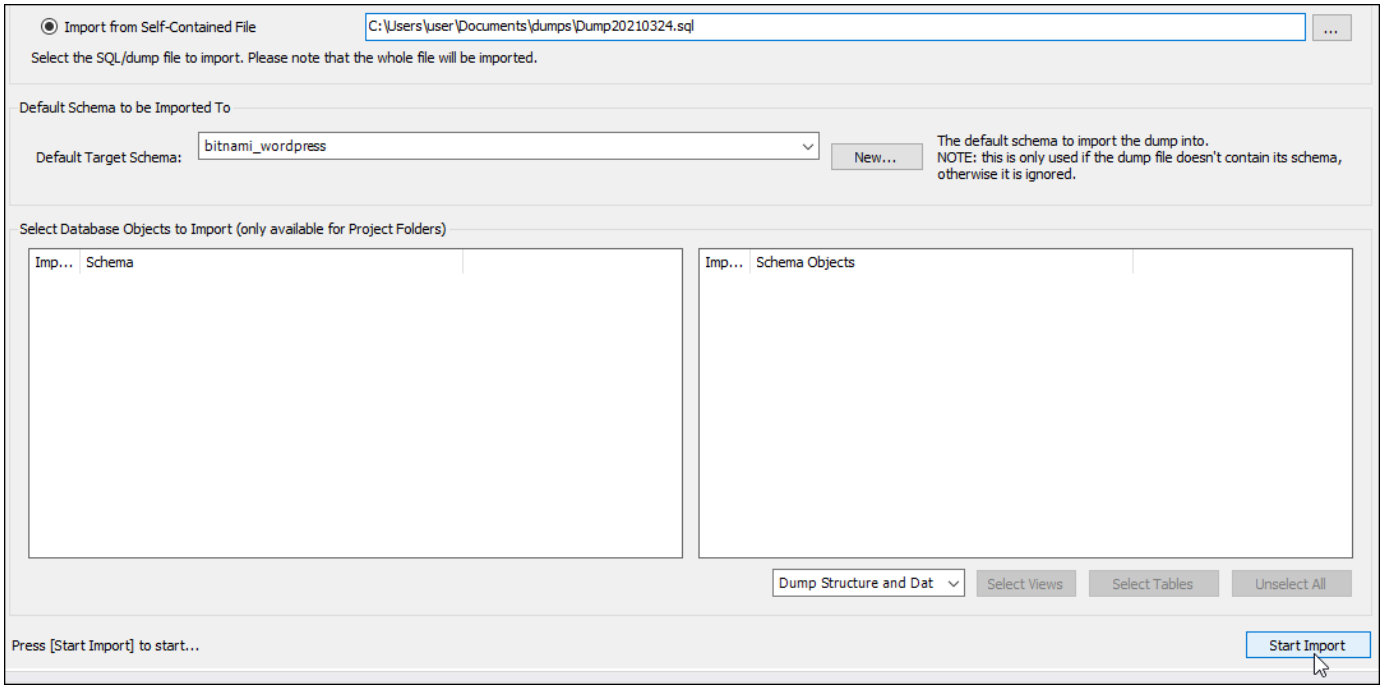


6. Geben Sie den Namen des Schemas in das Fenster Erstellen Sie ein Schema, das angezeigt wird, ein.

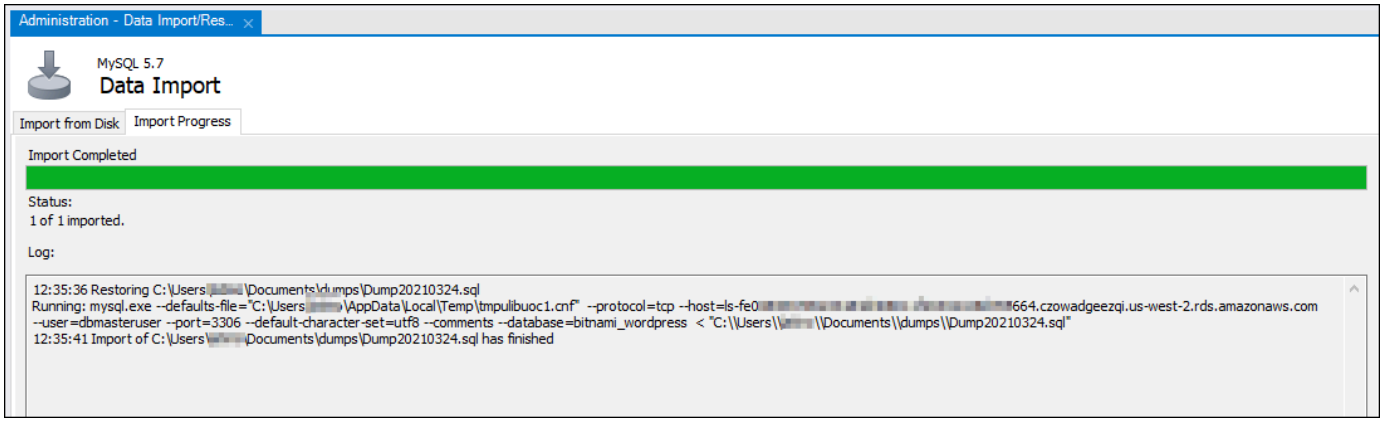
> **Note**
>
> In diesem Beispiel geben wir `bitnami_wordpress` ein, weil dies ist der Name der Datenbanktabelle ist, die wir exportiert haben.



7. Wählen Sie Import starten.



8. Warten Sie, bis der Import abgeschlossen ist, bevor Sie mit dem nächsten Abschnitt dieses Tutorials fortfahren.



Schritt 5: Testen Ihrer Anwendung und Abschluss der Migration

Zu diesem Zeitpunkt befinden sich Ihre Daten nun in Ihrer neuen MySQL-5.7-Datenbank. Konfigurieren Sie Ihre Anwendung in einer Vorproduktionsumgebung und testen Sie die Verbindung zwischen Ihrer Anwendung und Ihrer neuen MySQL-5.7-Datenbank. Wenn sich Ihre Anwendung wie erwartet verhält, fahren Sie mit der Änderung Ihrer Anwendung in der Produktionsumgebung fort.

Wenn Sie mit der Migration fertig sind, sollten Sie den öffentlichen Modus für Ihre Datenbanken deaktivieren. Sie können Ihre MySQL-5.6-Datenbank löschen, wenn Sie sicher sind, dass Sie sie nicht mehr benötigen. Sie sollten jedoch einen Snapshot Ihrer MySQL-5.6-Datenbank erstellen, bevor

Sie sie löschen. Während Sie dabei sind, sollten Sie auch einen Snapshot Ihrer neuen MySQL-5.7-Datenbank erstellen. Weitere Informationen finden Sie unter Erstellen eines Datenbank-Snapshots.

Einrichten und Konfigurieren von Plesk in Lightsail

Sie können einen Hosting Stack von Plesk mit den folgenden Funktionen in Amazon Lightsail einrichten.

- WordPress-Toolkit, Automatisierung in einer grafischen Benutzeroberfläche
- Unterstützung von Let's Encrypt für SSL-Zertifikate und Konfigurieren von verschlüsseltem (HTTPS) Datenverkehr auf einer einzelnen Instance
- FTP-Zugriff, um Dateien von und auf Ihre Instance zu übertragen
- Docker-Proxy-Regeln
- Webbasierte Verwaltungs- und Sicherheitstools, einschließlich Plesk-Firewall, Protokolle und ModSecurity

In diesem Handbuch erfahren Sie, wie Sie eine Plesk-Instance in Lightsail erstellen und wie Sie sich zum ersten Mal beim Plesk-Panel anmelden, indem Sie einen Benutzernamen und ein Passwort erstellen.

> **Important**
>
> Wenn nach dem Start Ihrer Plesk-Instance Probleme auftreten, rufen Sie die Plesk-Supportseite auf, um zu sehen, ob Updates auf der Instance installiert werden müssen. Weitere Informationen finden Sie im Plesk-Hilfecenter und Plesk-Updates im Plesk-Dokumentations- und Hilfeportal.

Eine Plesk-Instance erstellen

Führen Sie die folgenden Schritte aus, um eine Plesk-Instance in Lightsail zu erstellen.

1. Melden Sie sich bei der Lightsail-Konsole unter https://lightsail.aws.amazon.com/ an.
2. Wählen Sie auf der Registerkarte Instances der Lightsail-Startseite Instances erstellen
3. Wählen Sie den Speicherort aus, an dem Sie Ihre Instance erstellen möchten.

Wählen Sie AWS-Region und Availability Zone ändern aus, um den Standort der Instance zu ändern.

4. Wählen Sie unter Apps + OS (Anwendungen und OS) die Option Plesk Hosting Stack on Ubuntu (Plesk Hosting Stack auf Ubuntu) aus.
5. Wählen Sie Ihren Instance-Plan aus.

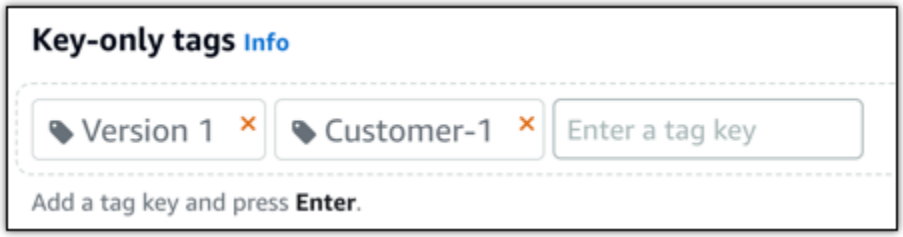
> **Note**
>
> Plesk wird im Rahmen des Lightsail-Plans für 3,50 USD pro Monat nicht unterstützt.

6. Geben Sie einen Namen für Ihre Instance ein.

   Ressourcennamen:

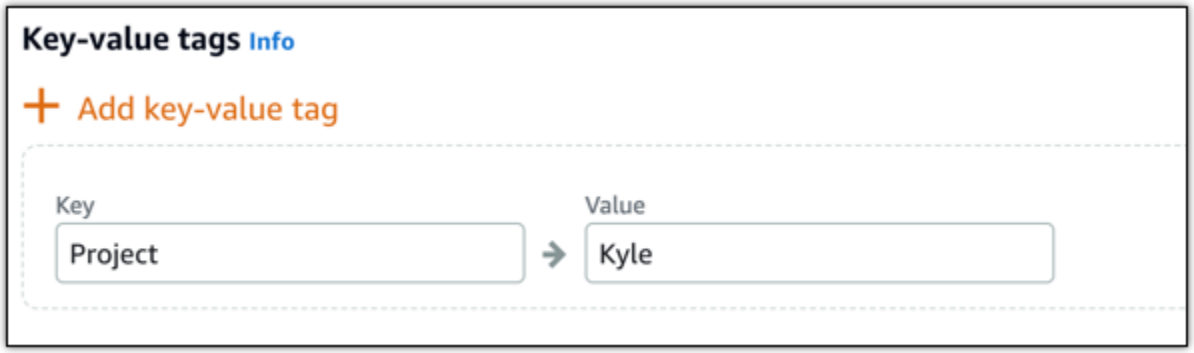
   - Muss innerhalb jeder AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
   - Muss zwischen 2 und 255 Zeichen enthalten.
   - Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
   - Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.
7. Wählen Sie eine der folgenden Optionen, um Ihrer Instance Tags hinzuzufügen:

   - Add key-only tags (Nur-Schlüssel-Tags hinzufügen) oder Edit key-only tags (Nur-Schlüssel-Tags bearbeiten) (wenn bereits Tags hinzugefügt wurden). Geben Sie Ihren neuen Tag in das Textfeld des Tag-Schlüssels ein und drücken Sie EINGABE. Wählen Sie Save (Speichern), wenn Sie mit der Eingabe Ihrer Tags fertig sind und sie hinzufügen möchten, oder wählen Sie Cancel (Abbrechen), um sie nicht hinzuzufügen.

   - Erstellen Sie ein Schlüssel-Wert-Tag, geben Sie dann einen Schlüssel in das Textfeld Key (Schlüssel) und einen Wert in das Textfeld Value (Wert) ein. Wählen Sie Save (Speichern) aus, wenn Sie mit der Eingabe Ihrer Tags fertig sind, oder wählen Sie Cancel (Abbrechen) aus, um sie nicht hinzuzufügen.

Schlüssel-Wert-Tags können nur vor dem Speichern hinzugefügt werden. Um mehr als ein Schlüssel-Wert-Tag hinzuzufügen, wiederholen Sie die vorherigen Schritte.



> **Note**
>
> Weitere Informationen zu Nur-Schlüssel- und Schlüssel-Wert-Tags finden Sie unter Tags.

8. Wählen Sie Create instance (Instance erstellen).

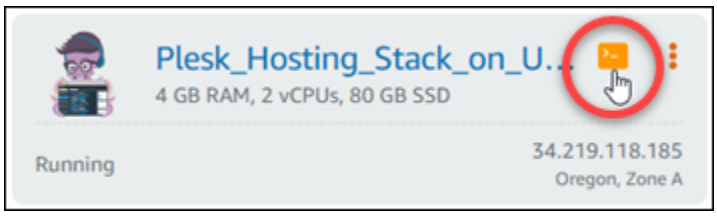
Die Instance benötigt nach dem Erstellen einige Minuten, bis sie bereitgestellt und verfügbar ist.

> **Note**
>
> Wenn Sie Plesk für das Web-Hosting auf Amazon Lightsail verwenden möchten, müssen Sie Ihrer Instance eine statische IP-Adresse anfügen. Um eine statische IP-Adresse anzufügen, müssen Sie die Instance in Lightsail neu starten, bevor Sie sich dort zum ersten Mal anmelden können.

Einen Benutzernamen und ein Passwort für Ihre Plesk-Instance konfigurieren

Führen Sie die folgenden Schritte aus, um einen Benutzernamen und ein Passwort für Ihre Plesk-Instance zu konfigurieren, und melden Sie sich zum ersten Mal im Plesk-Panel an.

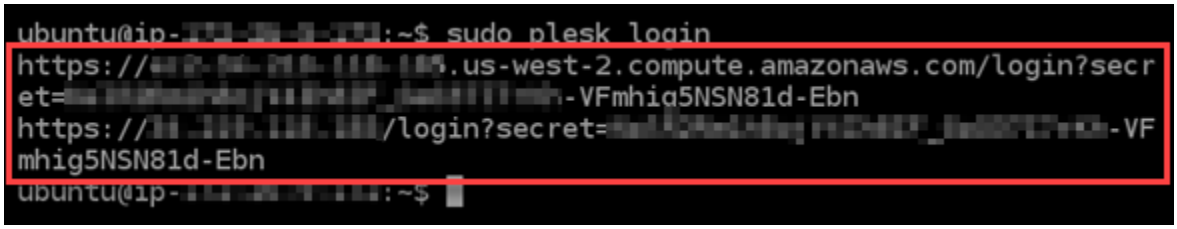
1. Wählen Sie auf der Registerkarte Instances der Lightsail-Startseite das SSH-Schnellverbindungssymbol für die Plesk-Instance aus, die Sie einrichten möchten.



2. Geben Sie den folgenden Befehl ein.

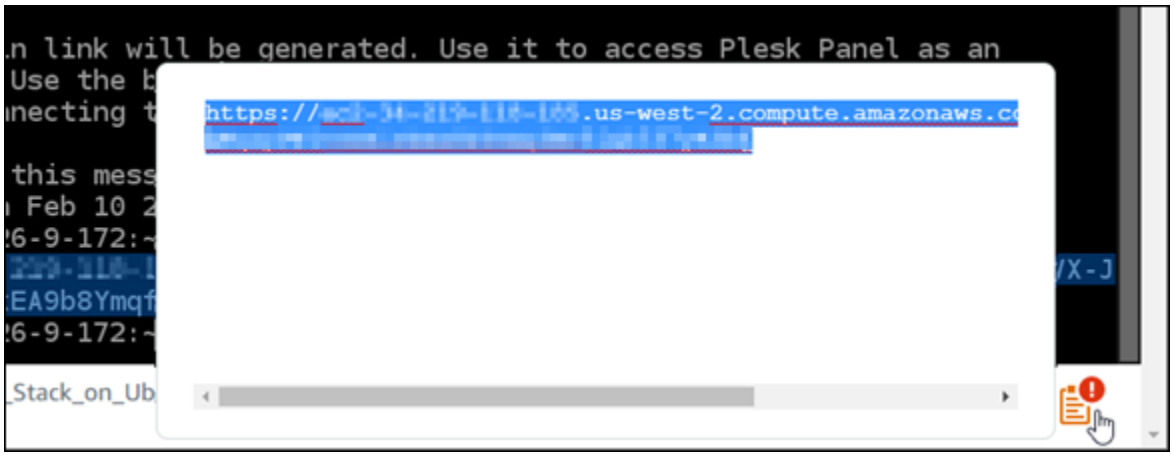
```
sudo plesk login | grep -v internal:8
```

Sie sollten ein Ergebnis ähnlich dem folgenden Beispiel erhalten:



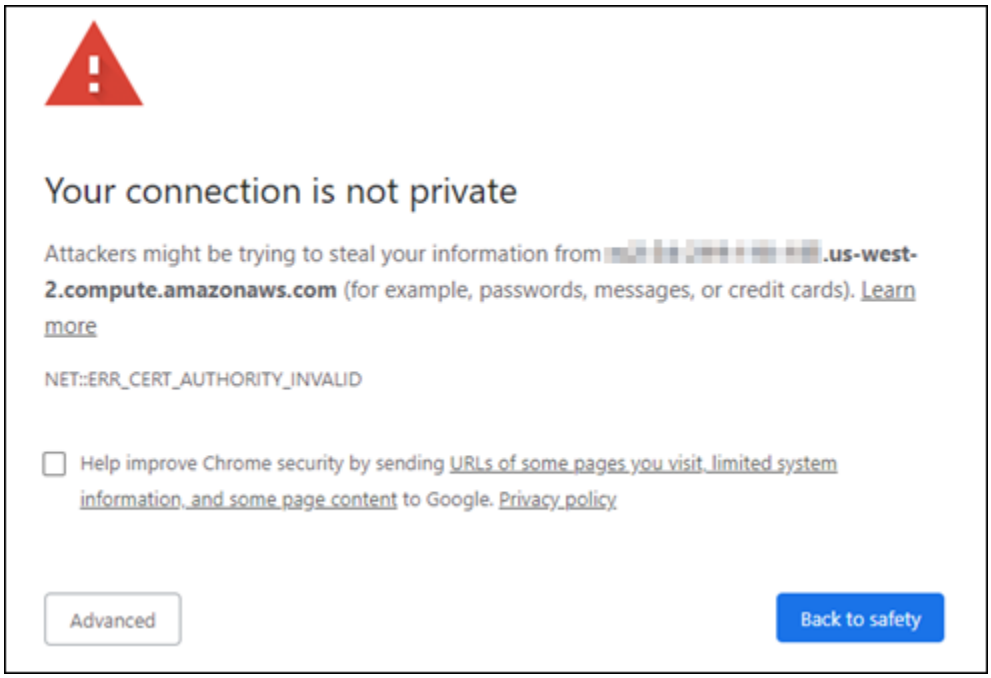
> **Important**
>
> Wenn Sie kürzlich eine statische IP an Ihre Plesk-Instance angehängt haben, erhalten Sie möglicherweise eine einmalige Anmelde-URL, die die alte öffentliche IP-Adresse verwendet. Starten Sie die Instance neu und führen Sie den obigen Befehl erneut aus, um eine einmalige Anmelde-URL zu erhalten, die die neue statische IP-Adresse verwendet.

3. Markieren Sie die URL, die im browserbasierten SSH-Fenster angezeigt wird, wählen Sie dann das Zwischenablage-Symbol und kopieren Sie die URL in die lokale Zwischenablage.



4. Öffnen Sie ein neues Browserfenster und navigieren Sie zu der URL, die Sie kopiert haben.

Möglicherweise warnt Ihr Browser Sie davor, dass Ihre Verbindung nicht privat bzw. sicher ist oder dass ein Sicherheitsrisiko besteht. Dies geschieht, weil Ihre Plesk-Instance noch nicht über eine SSL/TLS-Zertifikat verfügt. Je nach verwendetem Browser kann die Eingabeaufforderung anders als im folgenden Beispiel aussehen.

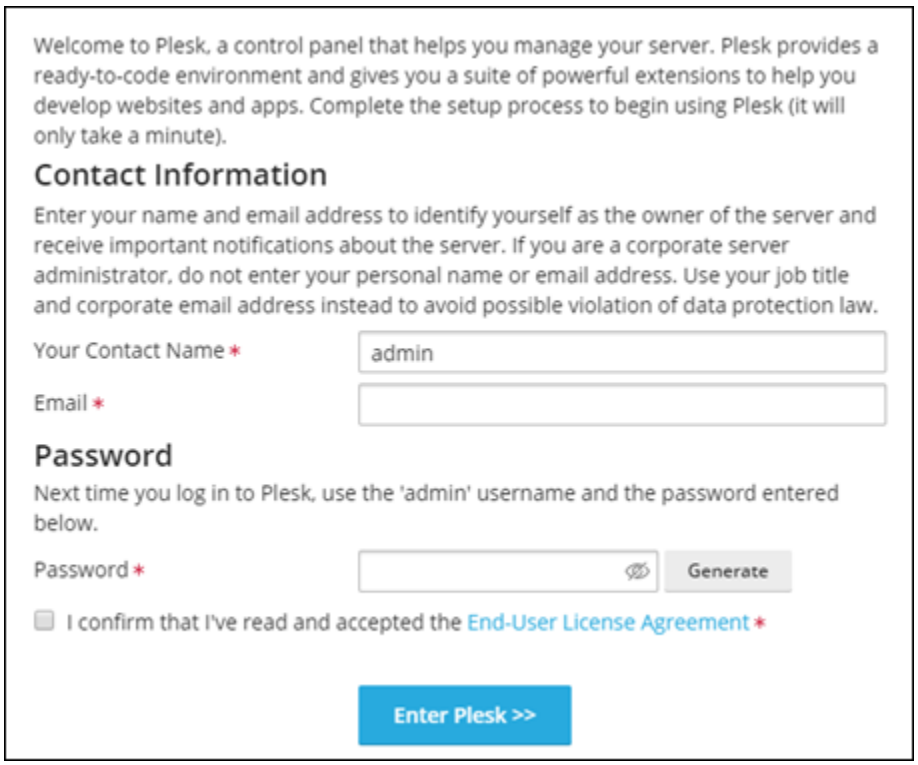


5. Führen Sie je nach verwendetem Browser einen der folgenden Schritte aus:

   - Chrome: Wählen Sie Advanced (Erweitert) und dann Proceed (Fortfahren), um zur Plesk-Einrichtungsseite zu wechseln.
   - Edge: Wählen Sie Details und dann Go on to the webpage (Not recommended) (Zur Webseite wechseln (Nicht empfohlen)), um zur Plesk-Einrichtungsseite zu wechseln.
   - Firefox: Wählen Sie Advanced (Erweitert) und Accept the Risk and Continue (Risiko akzeptieren und Fortfahren), um zur Plesk-Einrichtungsseite zu wechseln.
   - Internet Explorer: Wählen Sie More information (Weitere Informationen) und dann Go on to the webpage (Not recommended) (Zur Webseite wechseln (nicht empfohlen)), um zur Plesk-Einrichtungsseite zu wechseln.

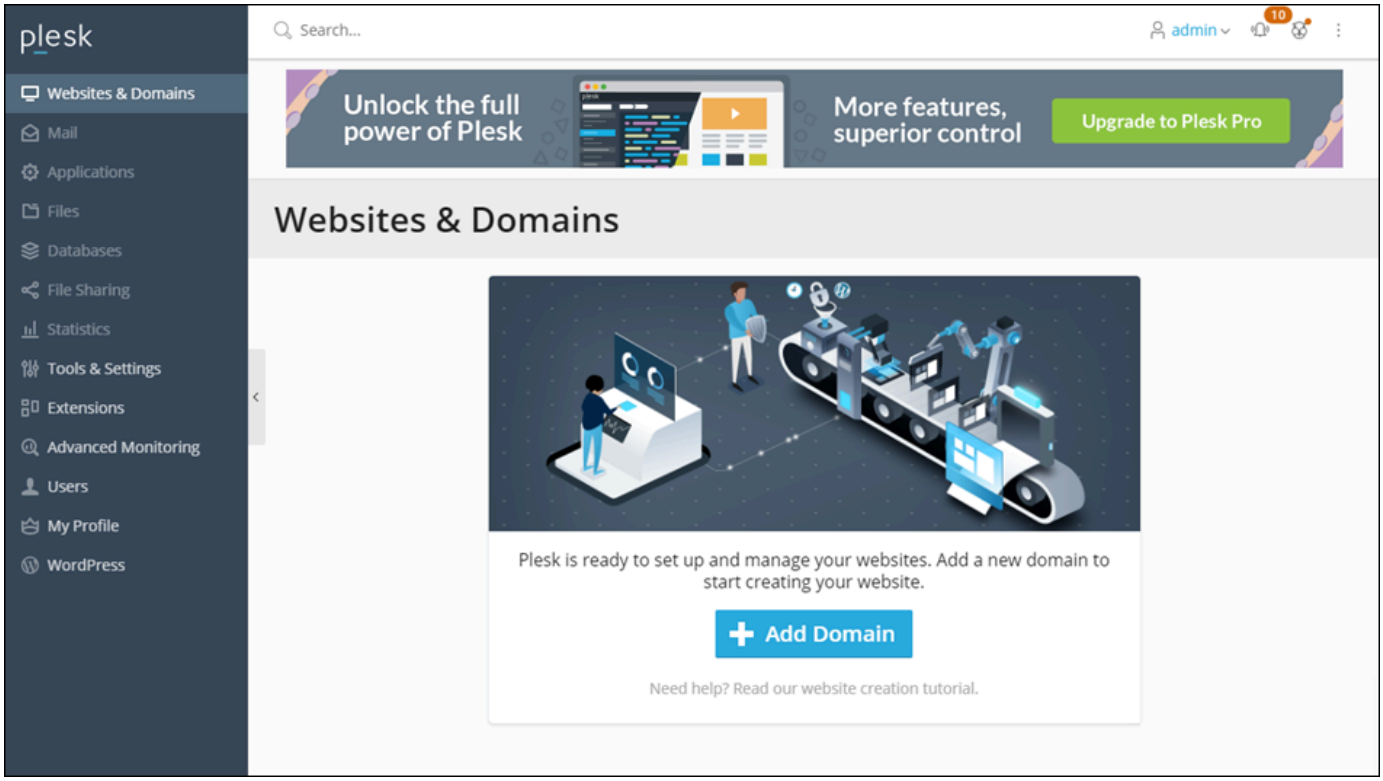
6. Geben Sie Ihren Kontaktnamen, Ihre E-Mail-Adresse und Ihr Passwort ein.

   Auf dieser Seite können Sie den standardmäßigen `admin`-Kontaktnamen ändern, wenn Sie einen anderen verwenden möchten. Dies ist jedoch nur der Anzeigename. Ihr Benutzername für die Anmeldung bei Plesk lautet weiterhin `admin`.



7. Bestätigen Sie, dass Sie die Endbenutzer-Lizenzvereinbarung akzeptieren, und wählen Sie Enter Plesk (Plesk öffnen).

   Sie werden im Plesk-Panel angemeldet, wo Sie Ihre Domain hinzufügen und mit der Verwaltung Ihrer Websites beginnen können.

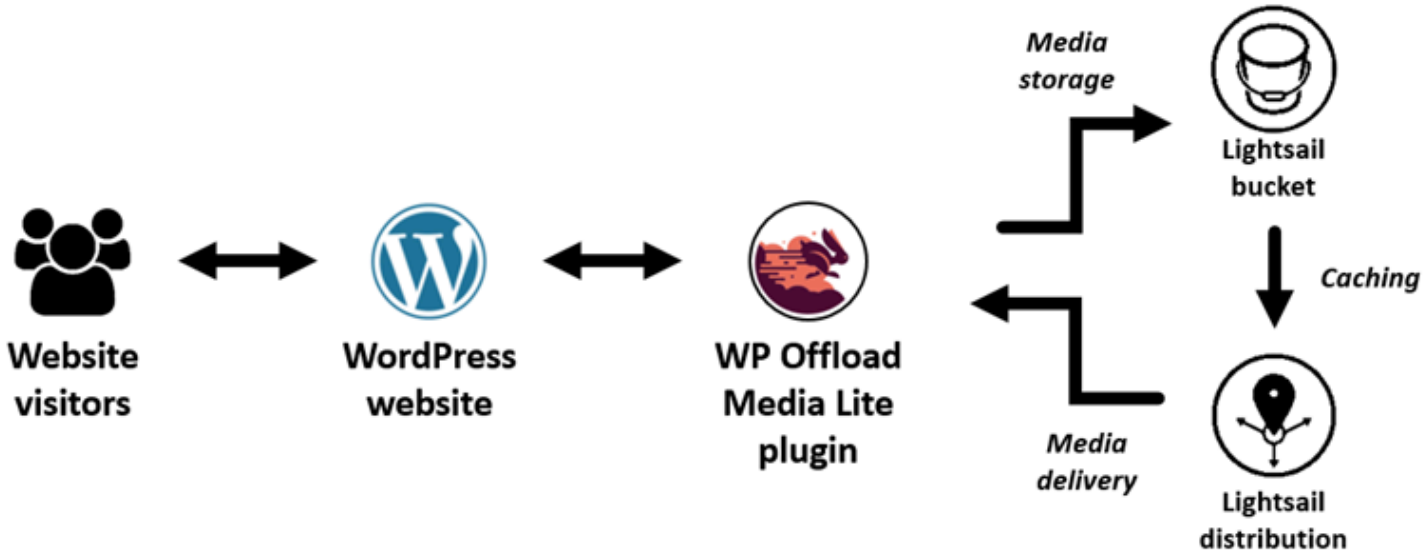


Wenn Sie sich später erneut anmelden müssen, navigieren Sie einfach zu `https://PublicIPAddress:8443`. Ersetzen Sie *`PublicIPAddress`* durch die öffentliche IP-Adresse oder die statische IP-Adresse Ihrer Instance. Zum Beispiel `https://192.0.2.0/:8443`. Geben Sie dann den Benutzernamen und das Passwort ein, die Sie zuvor für die Anmeldung im Plesk-Panel erstellt haben.

Weitere Informationen zur Verwendung von Plesk finden Sie unter Erste Schritte mit dem Verwalten von Websites in Plesk im Plesk-Dokumentations- und Hilfeportal.

Tutorial: Verwenden eines Lightsail-Buckets mit einer Netzwerkverteilung für die Bereitstellung von Inhalten

In diesem Tutorial werden die Schritte beschrieben, die erforderlich sind, um Ihren Amazon Lightsail-Bucket als Ursprung einer Lightsail-Content-Delivery-Network (CDN)-Verteilung zu konfigurieren. Außerdem wird beschrieben, wie Sie Ihre WordPress Website so konfigurieren, dass Medien (wie Bilder und Filmdateien) in Ihrem Bucket hochgeladen und gespeichert und Medien aus Ihrer Verteilung bereitgestellt werden. Ein Beispiel für diese Vorgehensweise ist die Nutzung des Plugins „WP Offload Media Lite“. Das folgende Diagramm verdeutlicht dieses Konzept.



Das Speichern von Website-Medien in einem Lightsail-Bucket führt dazu, dass Ihre Instance diese Dateien nicht speichern und bereitstellen muss. Das Zwischenspeichern und Bereitstellen von Medien aus einer Lightsail-Verteilung beschleunigt die Bereitstellung dieser Dateien an Ihre Website-Besucher und kann die allgemeine Website-Leistung verbessern. Weitere Informationen zu Verteilungen finden Sie unter Netzwerkverteilungen für die Bereitstellung von Inhalten. Weitere Informationen zu Buckets finden Sie unter Objektspeicher.

Inhalt

Schritt 1: Erfüllen der Voraussetzungen

Erfüllen Sie die folgenden Voraussetzungen, wenn dies noch nicht geschehen ist:

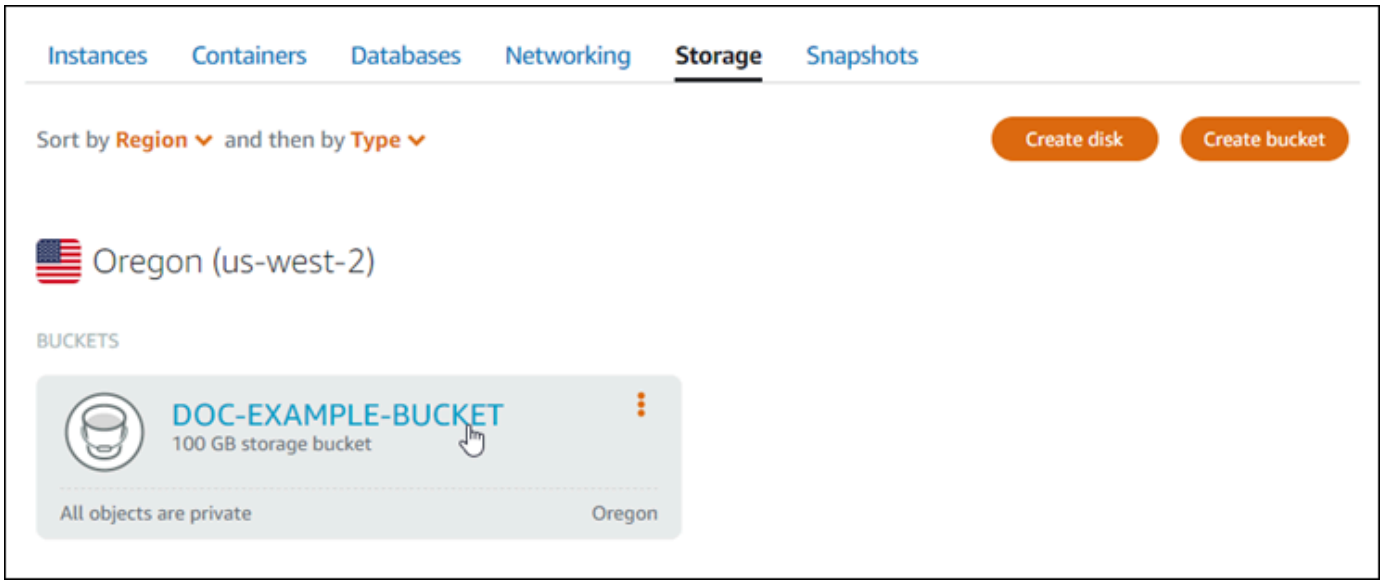
- Erstellen und konfigurieren Sie eine WordPress Instance in Lightsail und rufen Sie das Passwort ab, um sich beim Verwaltungs-Dashboard anzumelden. Weitere Informationen finden Sie unter Tutorial: Starten und Konfigurieren einer WordPress Instance in Amazon Lightsail.

- Erstellen Sie einen Bucket im Lightsail-Objektspeicherdienst. Weitere Informationen finden Sie unter Erstellen von Buckets in Lightsail.

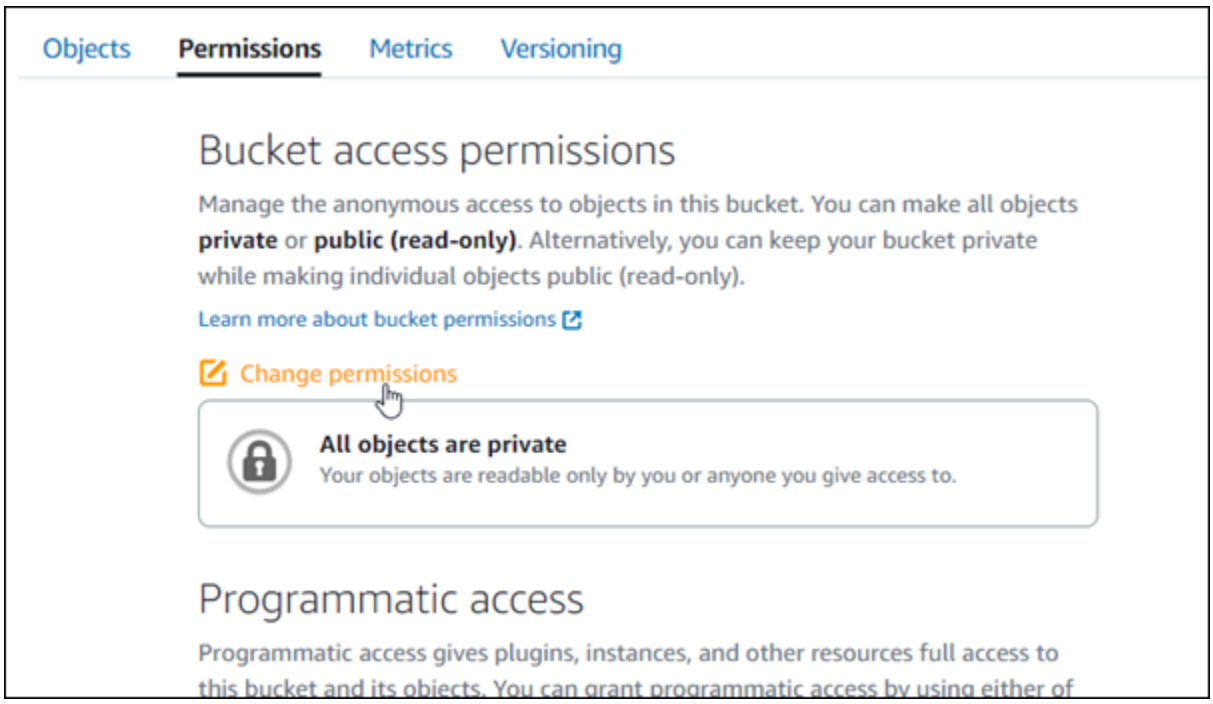
Schritt 2: Ändern der Bucket-Berechtigungen

Führen Sie das folgende Verfahren aus, um Ihrer WordPress Instance und dem WP Offload Media Lite-Plugin Zugriff auf Ihren Bucket zu gewähren. Die Berechtigungen Ihres Buckets müssen auf Einzelne Objekte können öffentlich gemacht werden (schreibgeschützt) eingestellt werden. Sie müssen Ihre WordPress Instance auch an Ihren Bucket anfügen. Weitere Informationen zu Bucket-Berechtigungen finden Sie unter Bucket-Berechtigungen.

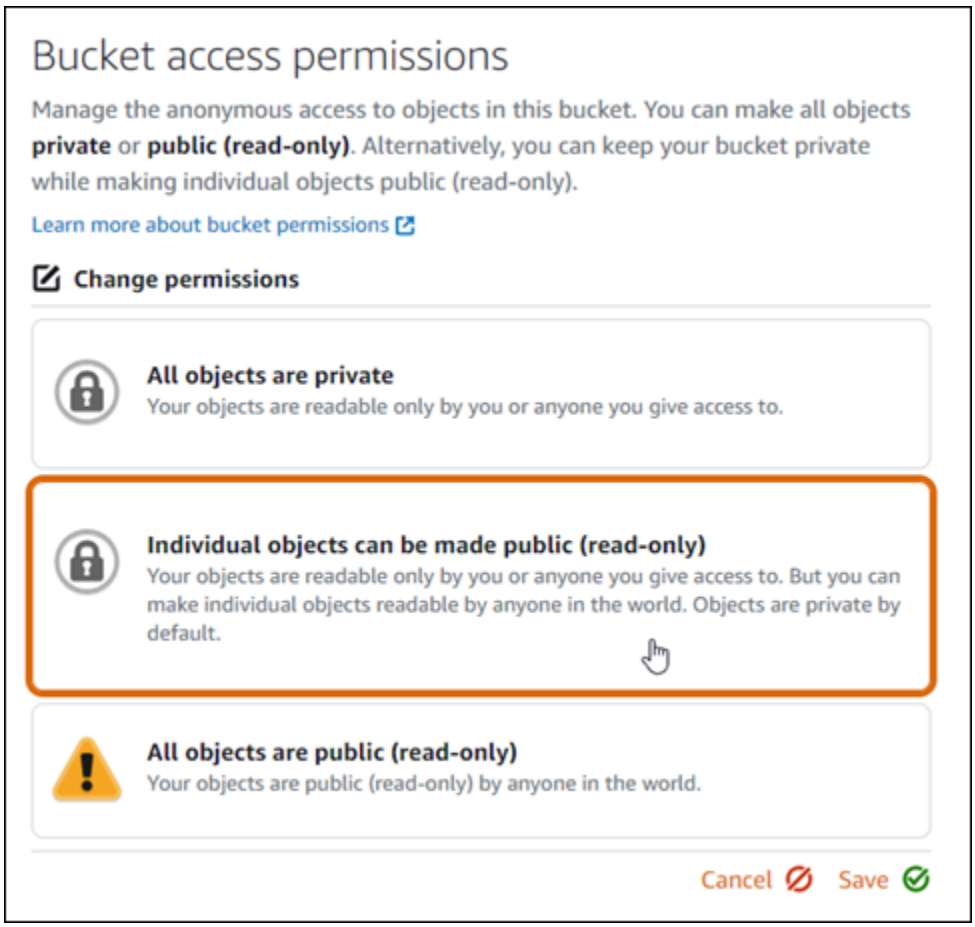
1. Melden Sie sich bei der Lightsail-Konsole an.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Speicher aus.
3. Wählen Sie den Namen des Buckets aus, den Sie mit Ihrer WordPress Website verwenden möchten.



4. Wählen Sie die Registerkarte Berechtigungen auf der Seite Bucket-Verwaltung aus.
5. Wählen Sie Ändern von Berechtigungen unter Abschnitt Zugriffsberechtigungen für Buckets der Seite.

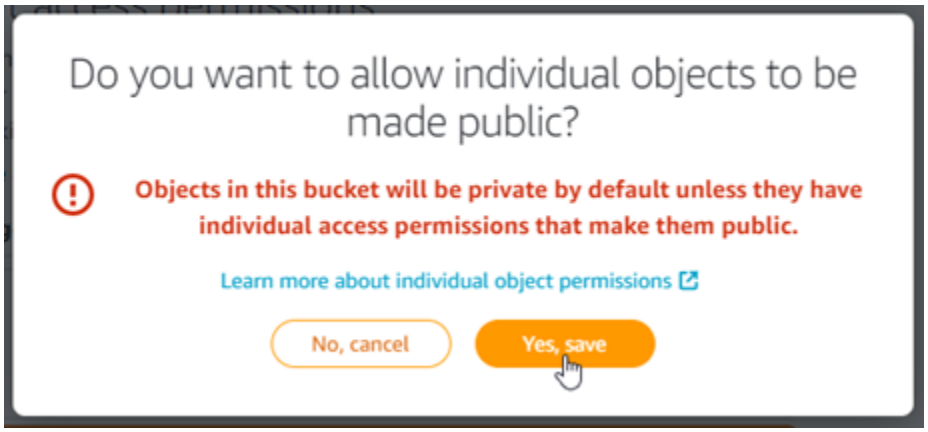


6. Wählen Sie Einzelne Objekte können öffentlich und schreibgeschützt gemacht werden.



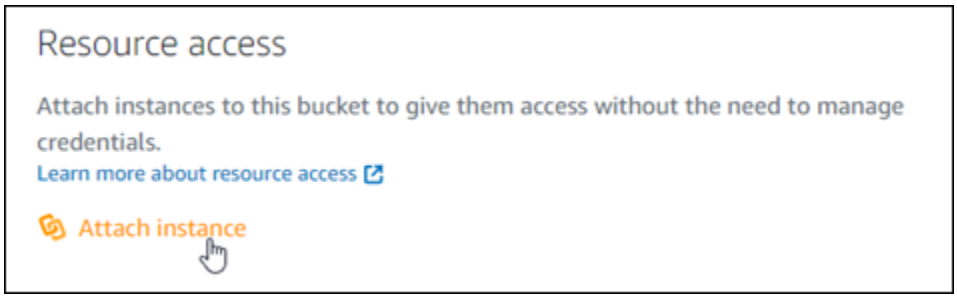
7. Wählen Sie Speichern.

8. Wählen Sie in der angezeigten Bestätigungsaufforderung Ja, speichern.

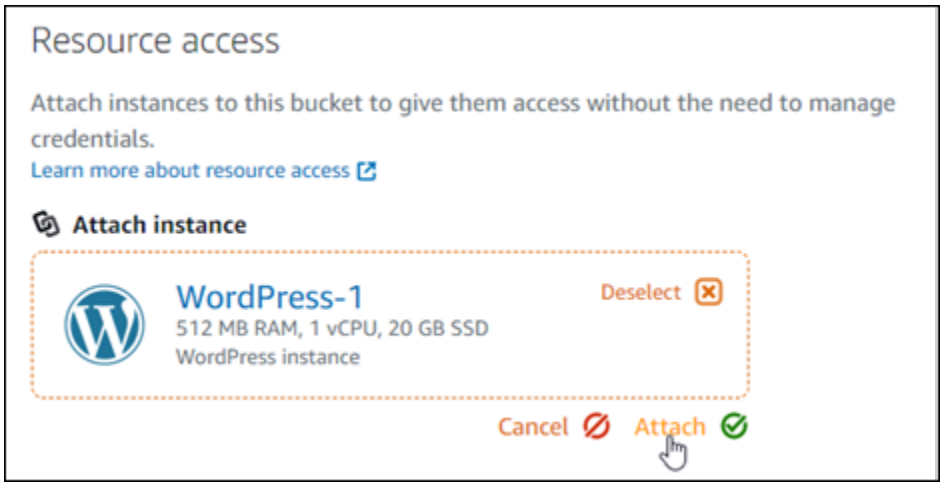


Nach einigen Augenblicken wird Ihr Bucket so konfiguriert, dass ein individueller Objektzugriff möglich ist. Dadurch wird sichergestellt, dass Objekte, die von Ihrer WordPress Website mit dem Offload Media Lite-Plugin in Ihren Bucket hochgeladen werden, für Ihre Kunden lesbar sind.

9. Scrollen Sie zum Abschnitt Zugriff auf Ressourcen der Seite und wählen Sie Instance hinzufügen.



10. Wählen Sie den Namen Ihrer WordPress Instance im daraufhin angezeigten Dropdown-Menü und dann Anfügen aus.



Nach einigen Augenblicken ist Ihre WordPress Instance mit Ihrem Bucket verbunden. Dadurch erhält Ihre WordPress Instance Zugriff auf die Verwaltung Ihres Buckets und seiner Objekte.

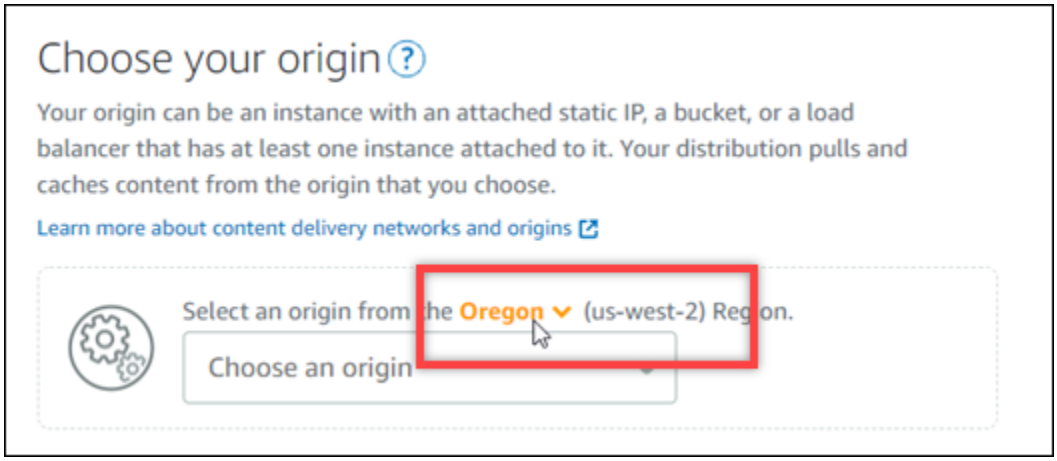
Schritt 3: Erstellen einer Verteilung mit einem Bucket als Ursprung

Führen Sie das folgende Verfahren aus, um eine Lightsail-Verteilung zu erstellen und Ihren Lightsail-Bucket als Ursprung auszuwählen.

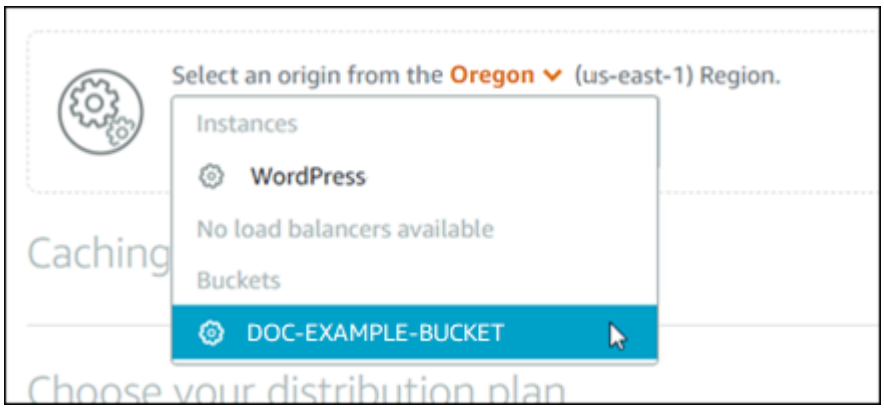
1. Wählen Sie im oberen Navigationsmenü der Lightsail-Konsole Home aus.
2. Wählen Sie auf der Lightsail-Startseite die Registerkarte Networking (Netzwerk).
3. Wählen Sie Verteilung erstellen aus.

4. Im Abschnitt Wählen Sie Ihren Ursprung der Seite wählen Sie die AWS-Region , in der Sie Ihren Bucket erstellt haben.

   Verteilungen sind globale Ressourcen. Sie können auf einen Bucket in jeder verweisen AWS-Region und seinen Inhalt global verteilen.

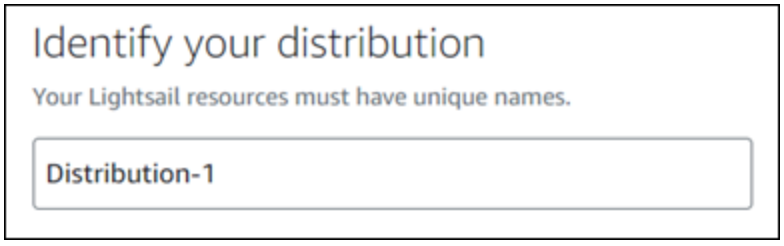


5. Wählen Sie Ihren Bucket als Ursprung.



> **Note**
>
> Die Berechtigungen Ihres Buckets müssen auf Einzelne Objekte können öffentlich gemacht werden (schreibgeschützt) eingestellt werden. Nur einzelne Objekte, die öffentlich sind, werden von der Verteilung zwischengespeichert und bedient. Wenn Sie einen Bucket als Ursprung einer Verteilung auswählen, werden die Optionen zum Angeben der Ursprungsprotokollrichtlinie, des Cache-Verhaltens, des Standardverhaltens sowie der Verzeichnis- und Dateiüberschreibungen nicht verfügbar und können nicht bearbeitet werden. Die Ursprungsprotokollrichtlinie ist standardmäßig HTTP für Buckets und das Caching-Verhalten standardmäßig auf Alles zwischenspeichern. Sie können die fortschrittlichen Cache-Einstellungen der Verteilung ändern, nachdem sie erstellt wurde.

6. Wählen Sie Ihren Verteilungsplan aus.
7. Geben Sie einen Namen für Ihre Verteilung ein.



Verteilungsnamen:

- Muss in jedem AWS-Region in Ihrem Lightsail-Konto eindeutig sein.
- Müssen 2–255 Zeichen enthalten.
- Muss mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
- Kann alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche enthalten.

8. Wählen Sie Verteilung erstellen aus.

Ihre Verteilung wird nach wenigen Augenblicken erstellt. Wenn Ihre neue Verteilung einen Enabled-Status erreich, ist sie bereit, Objekte, die sich in Ihrem Bucket befinden, bereitzustellen und zwischenzuspeichern.

Schritt 4: Aktivieren benutzerdefinierter Domänen für Ihre Verteilung

Wenn Sie Ihre Verteilung erstellen, wird sie mit einer Standarddomäne konfiguriert, die ähnlich mit `123abc.cloudfront.net` ist. Sie können diese Standarddomäne als Quelle Ihrer Mediendateien angeben, wenn Sie das WP Offload Media Lite-Plugin konfigurieren. Es wird jedoch dringend empfohlen, eine benutzerdefinierte Domäne für Ihre Verteilung zu aktivieren. Die benutzerdefinierte Domäne, die Sie für Ihre Verteilung aktivieren, sollte eine Subdomäne der Domäne sein, die Sie mit Ihrer WordPress Website verwenden. Wenn Sie beispielsweise `mycustomdomain.com` mit Ihrer WordPress Website verwenden, können Sie die benutzerdefinierte Domain `media.mycustomdomain.com` mit Ihrer Verteilung verwenden. Die Verwendung derselben Domain- und Subdomain-Kombination zwischen Ihrer WordPress Website und Ihrer Verteilung trägt dazu bei, den Suchmaschinenoptimierungswert Ihrer Website zu verbessern.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Domäne für Ihre Verteilung zu konfigurieren:

1. Erstellen Sie ein Lightsail-SSL-/TLS-Zertifikat für Ihre Domain, um es mit Ihrer Verteilung zu verwenden. Lightsail-Verteilungen erfordern HTTPS, daher müssen Sie ein SSL-/TLS-Zertifikat für Ihre Domäne anfordern, bevor Sie es mit Ihrer Verteilung verwenden können. Weitere Informationen finden Sie unter Erstellen von SSL-/TLS-Zertifikaten für Ihre Verteilung.
2. Aktivieren Sie benutzerdefinierte Domänen für Ihre Verteilung, um Ihre Domäne mit Ihrer Verteilung zu verwenden. Um benutzerdefinierte Domänen zu aktivieren, müssen Sie das Lightsail-SSL-/TLS-Zertifikat angeben, das Sie für Ihre Domäne erstellt haben. Dadurch wird Ihre Domain zur Verteilung hinzugefügt und HTTPS aktiviert. Weitere Informationen finden Sie unter Aktivieren benutzerdefinierter Domains für Ihre Verteilung.

3. Fügen Sie einen Alias-Datensatz zur DNS-Zone Ihrer Domäne hinzu. Nachdem Sie den Alias-Datensatz hinzugefügt haben, werden Benutzer, die Ihre Domäne besuchen, über Ihre Verteilung weitergeleitet. Weitere Informationen finden Sie unter Verweisen Ihrer Domain auf eine Verteilung.

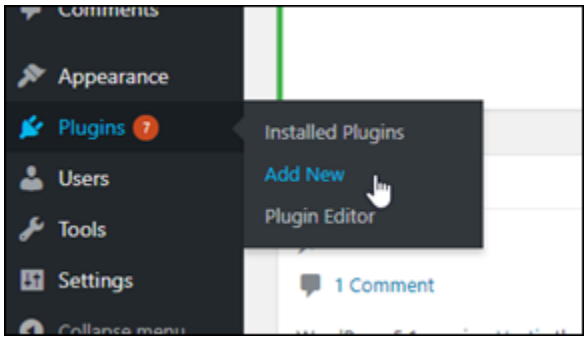
Schritt 5: Installieren des WP Offload Media Lite-Plugins auf Ihrer WordPress Website

Führen Sie das folgende Verfahren aus, um das WP Offload Media Lite-Plugin auf Ihrer WordPress Website zu installieren. Dieses Plugin kopiert automatisch Bilder, Videos, Dokumente und andere Medien, die über WordPressden Medien-Uploader von hinzugefügt wurden, in Ihren Lightsail-Bucket. Es kann auch so konfiguriert werden, dass Medien aus Ihrem Bucket über Ihre Lightsail-Verteilung bereitgestellt werden. Weitere Informationen finden Sie unter WP Offload Media Lite auf der WordPress Website .

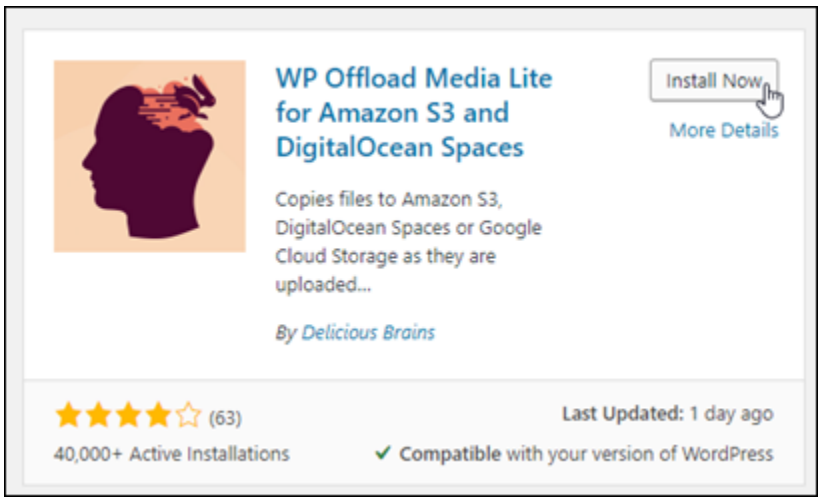
1. Melden Sie sich beim Dashboard Ihrer WordPress Website als Administrator an.

   Weitere Informationen finden Sie unter Abrufen des Anwendungsbenutzernamens und des Passworts für Ihre Bitnami-Instance in Amazon Lightsail.

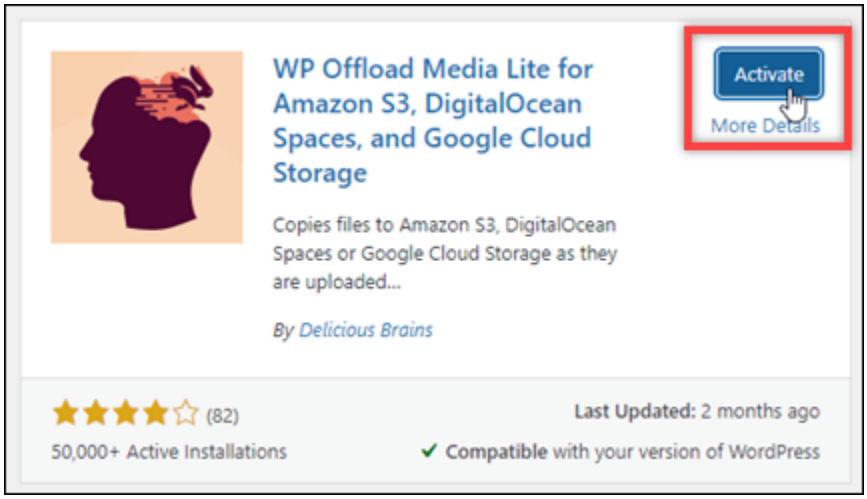
2. Pausieren Sie Plugins im linken Navigationsmenü und wählen Sie Add New (Neues auswählen).



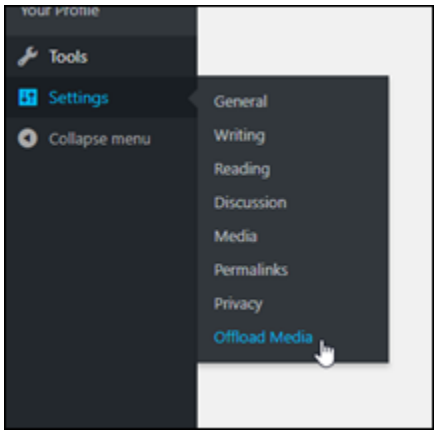
3. Suchen Sie nach WP Offload Media Lite.
4. Wählen Sie in den Suchergebnissen Install Now (Jetzt installieren) neben dem WP-Offload-Media-Plug-In aus.



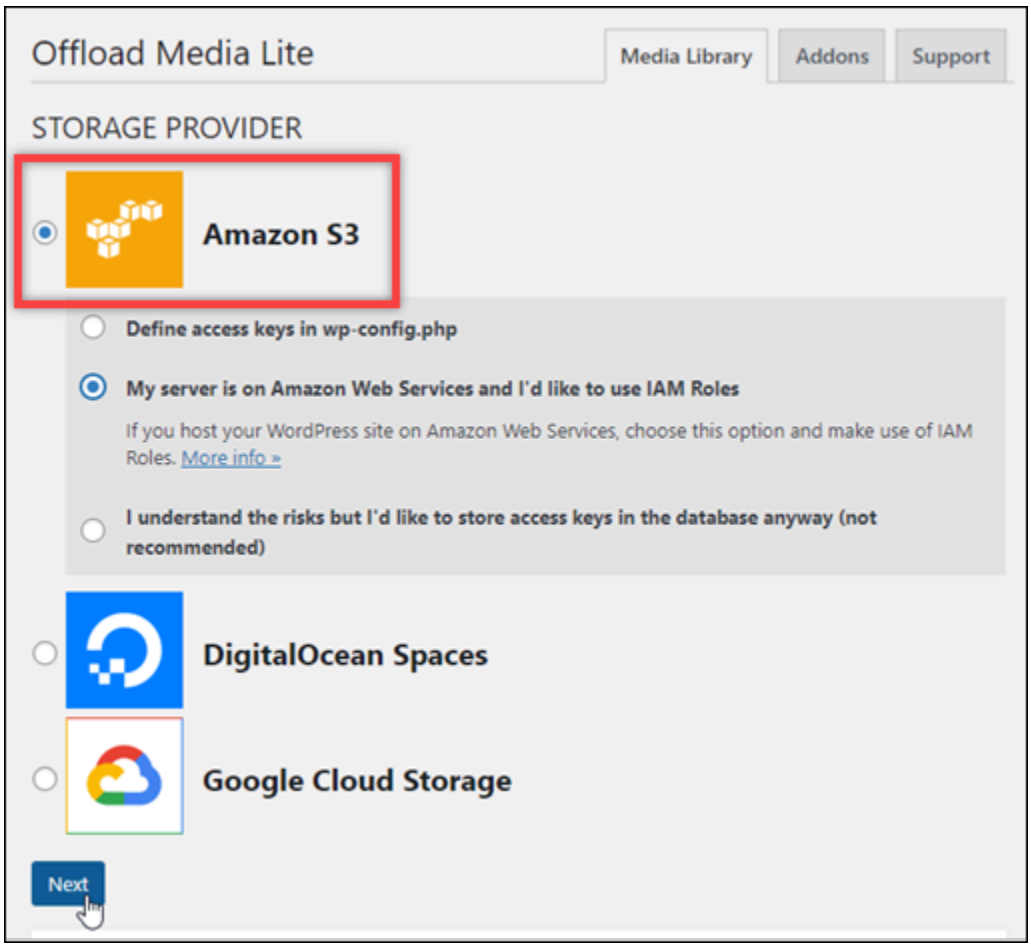
5. Wählen Sie Activate (Aktivieren) aus, nachdem das Plug-In installiert wurde.



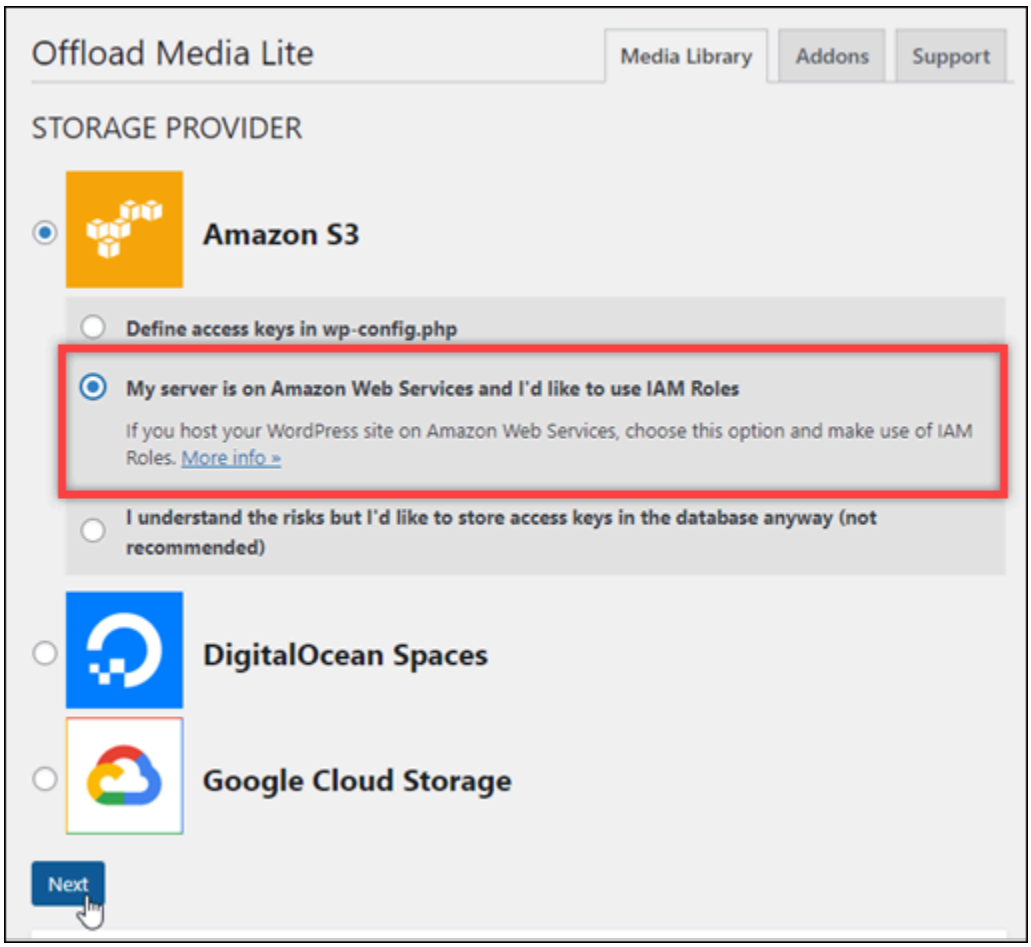
6. Wählen Sie im linken Navigationsmenü Settings (Einstellungen) und dann Offload Media aus.



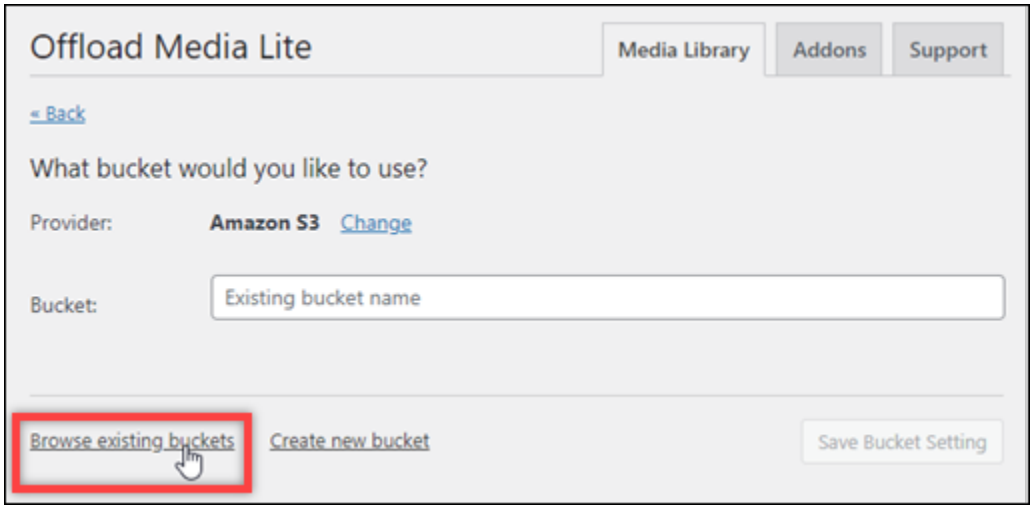
7. In der Seite Offload Media Lite wählen Sie Amazon S3 als Speicheranbieter.



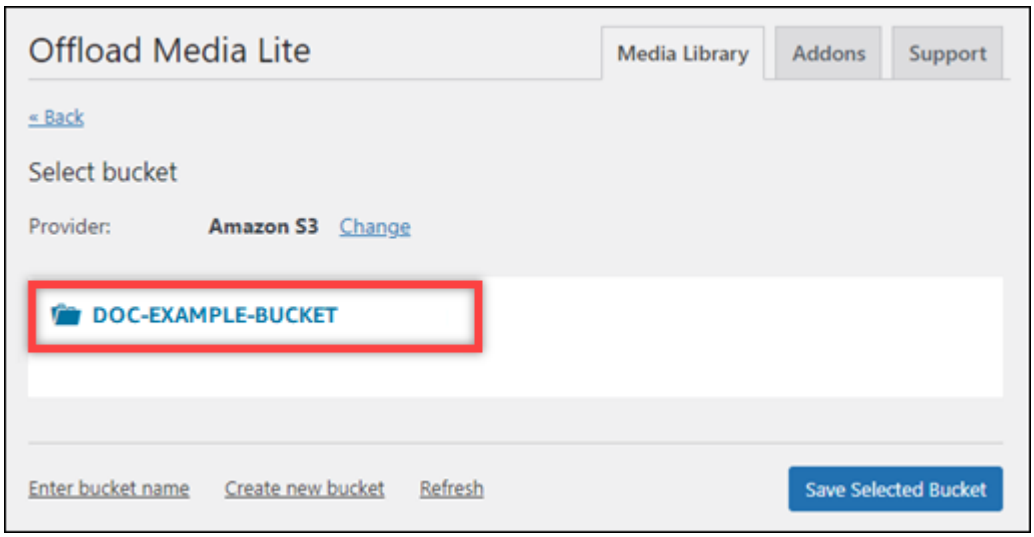
8. Klicken Sie auf Mein Server ist auf Amazon Web Services und ich möchte IAM-Rollen verwenden aus.



9. Wählen Sie Weiter aus.
10. Wählen Sie Durchsuchen vorhandener Buckets auf der Seite Welches Bucket möchten Sie verwenden?, die angezeigt wird.



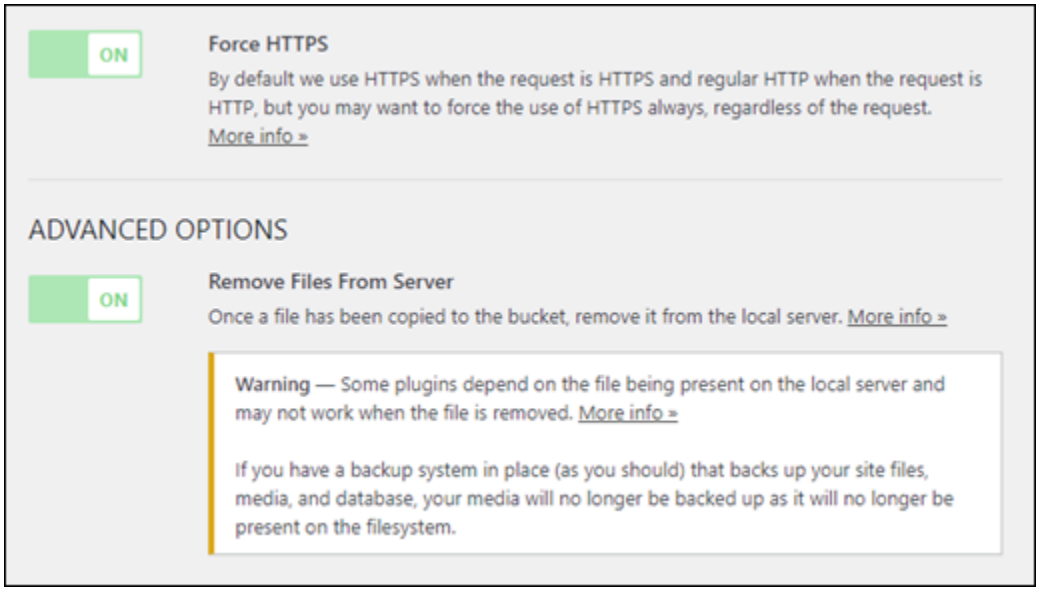
11. Wählen Sie den Namen des Buckets aus, den Sie für die Verwendung mit Ihrer WordPress Instance erstellt haben.



12. In der Seite Media-Lite-Einstellungen auslagern, die daraufhin angezeigt wird, aktivieren Sie HTTPS erzwingen und Dateien vom Server entfernen.

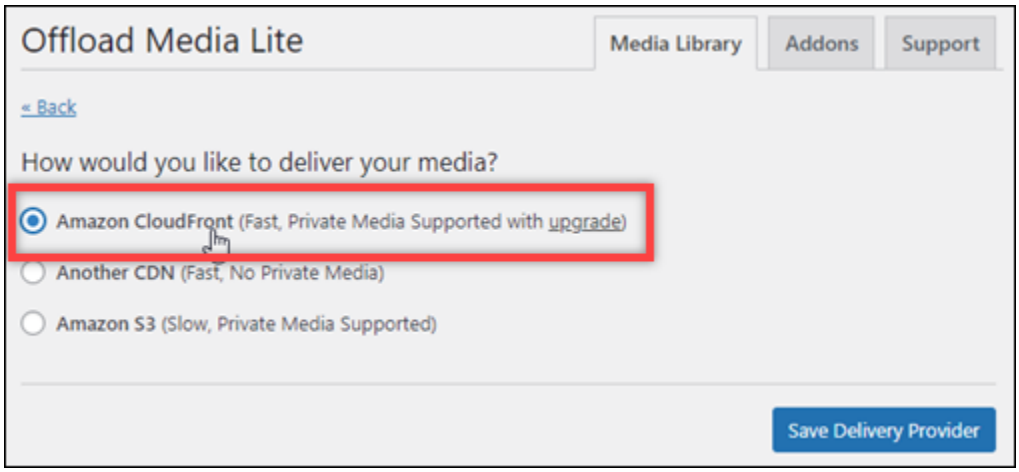
    - Die Einstellung HTTPS erzwingen muss aktiviert sein, da Lightsail-Buckets standardmäßig HTTPS verwenden, um Mediendateien bereitzustellen. Wenn Sie diese Funktion nicht aktivieren, werden Mediendateien, die von Ihrer WordPress Website in Ihren Lightsail-Bucket hochgeladen werden, nicht korrekt an Ihre Website-Besucher bereitgestellt.

      Die Einstellung Dateien vom Server entfernen stellt sicher, dass Medien, die in Ihren Lightsail-Bucket hochgeladen werden, nicht auch auf der Festplatte Ihrer Instance gespeichert werden. Wenn Sie diese Funktion nicht aktivieren, werden Mediendateien, die in Ihren Lightsail-Bucket hochgeladen werden, auch im lokalen Speicher Ihrer Instance gespeichert WordPress .



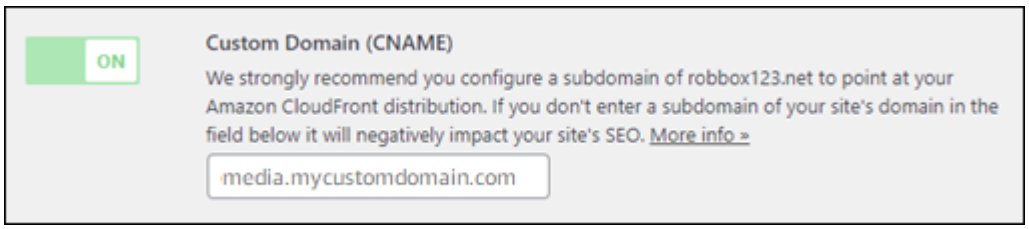
13. Im Abschnitt Lieferung der Seite wählen Sie Änderung neben dem Amazon-S3-Etikett.

14. Wählen Sie auf der daraufhin angezeigten Seite Wie möchten Sie Ihre Medien bereitstellen? die Option Amazon aus CloudFront.



15. Wählen Sie Anbieter für Zustellungen speichern aus.
16. In der Seite Media-Lite-Einstellungen auslagern, die daraufhin angezeigt wird, aktivieren Sie Benutzerdefinierte Domäne (CNAME). Geben Sie dann die Domain Ihrer Lightsail-Verteilung in das Textfeld ein. Dies könnte die Standarddomäne Ihrer Verteilung sein (z. B.

`123abc.cloudfront.net`) oder die benutzerdefinierte Domäne für Ihre Verteilung (z. B. `media.mycustomdomain.com`), wenn Sie sie aktiviert haben.



17. Wählen Sie Save Changes.

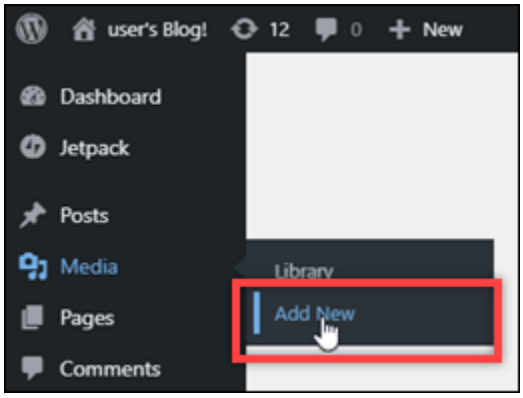
> **Note**
>
> Um später zur Seite Media-Lite-Einstellungen auslagern zurückzukehren, pausieren Sie Einstellungen im linken Navigationsmenü und wählen Sie Medien auslagern.

Ihre WordPress Website ist jetzt für die Verwendung des Media-Lite-Plugins konfiguriert. Wenn Sie das nächste Mal eine Mediendatei über hochladen WordPress, wird diese Datei automatisch in Ihren Lightsail-Bucket hochgeladen und von der Verteilung bedient. Fahren Sie mit dem nächsten Abschnitt dieses Tutorials fort, um die Konfiguration zu testen.

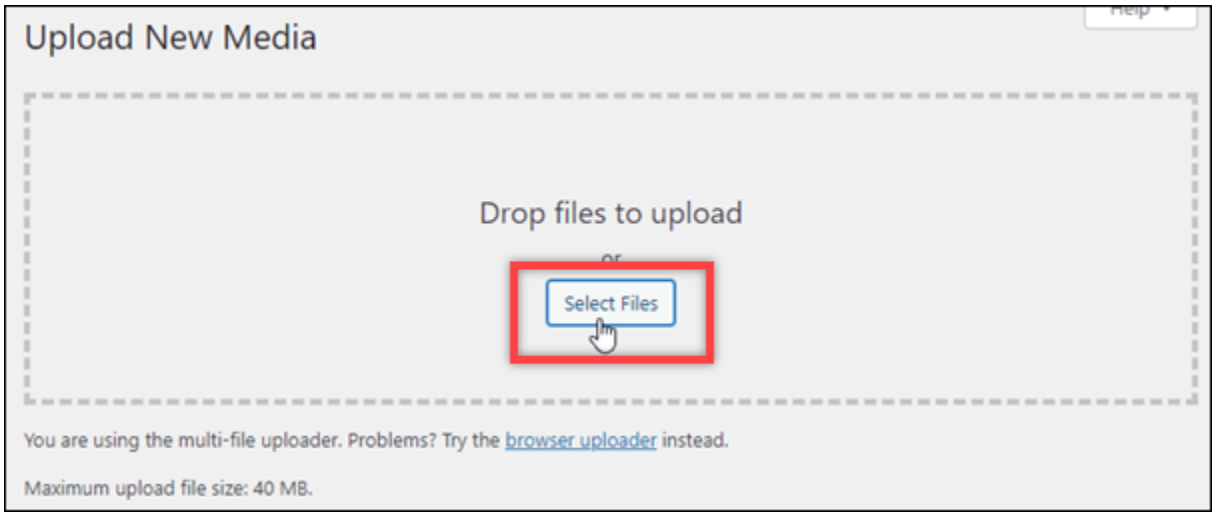
Schritt 6: Testen der Verbindung zwischen Ihrer WordPress Website und Ihrem Lightsail-Bucket und Ihrer Verteilung

Führen Sie das folgende Verfahren aus, um eine Mediendatei auf Ihre WordPress Instance hochzuladen und zu bestätigen, dass sie in Ihren Lightsail-Bucket hochgeladen und von Ihrer Verteilung bereitgestellt wird.

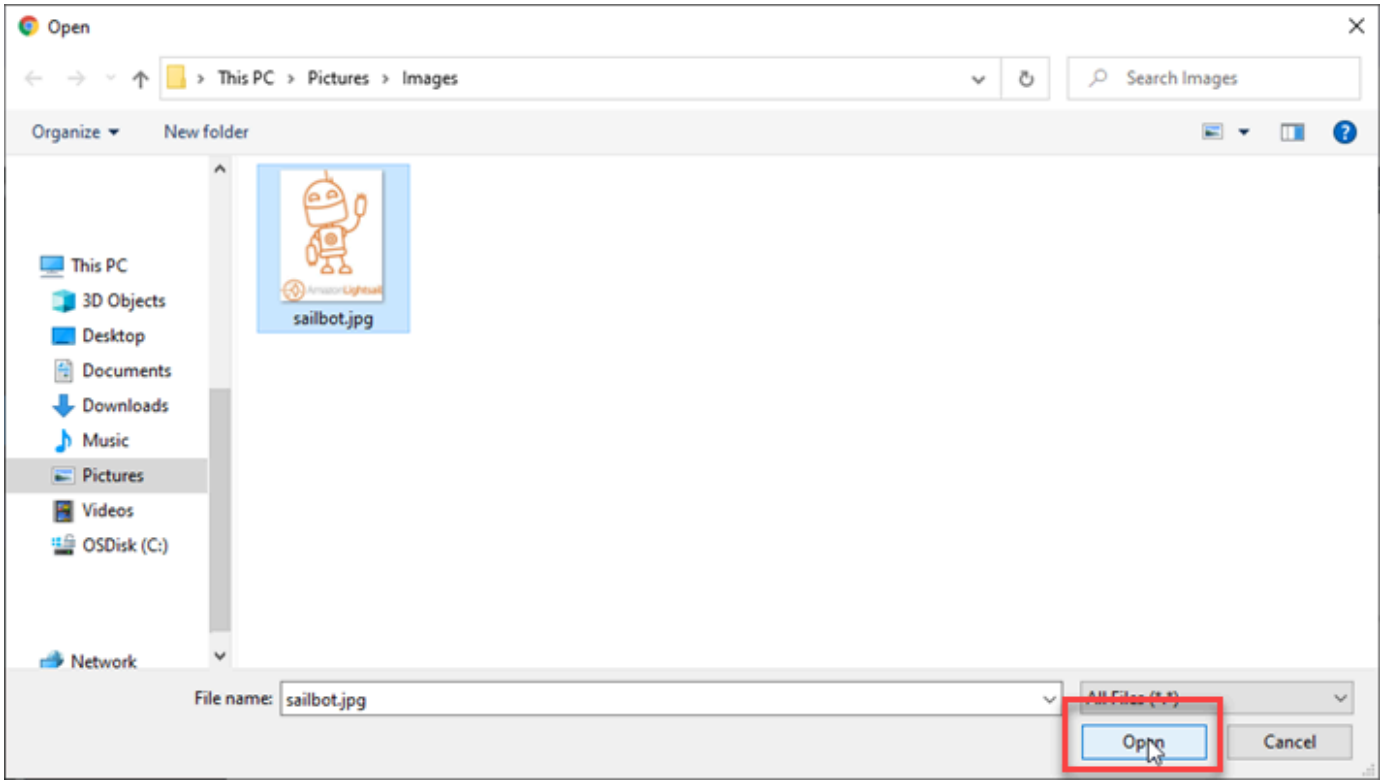
1. Pausieren Sie im linken Navigationsmenü des WordPress Dashboards auf Medien und wählen Sie Neu hinzufügen aus.



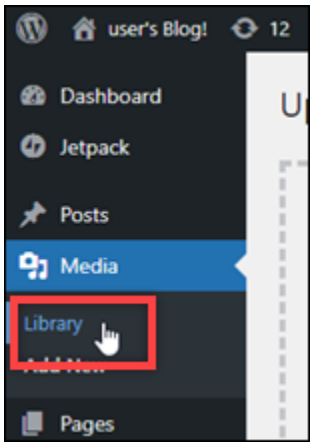
2. Wählen Sie Dateien auswählen auf der Seite Neue Medien uploaden die angezeigt wird.



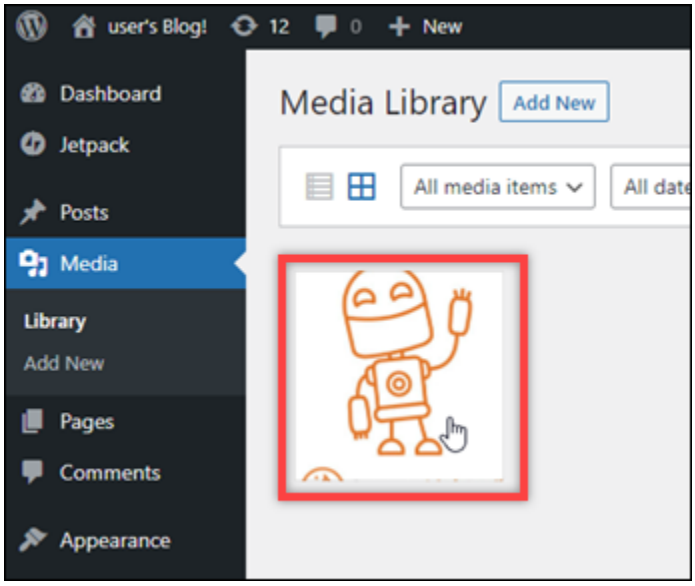
3. Wählen Sie eine Mediendatei aus, die von Ihrem lokalen Computer hochgeladen werden soll, und wählen Sie Öffnen aus.



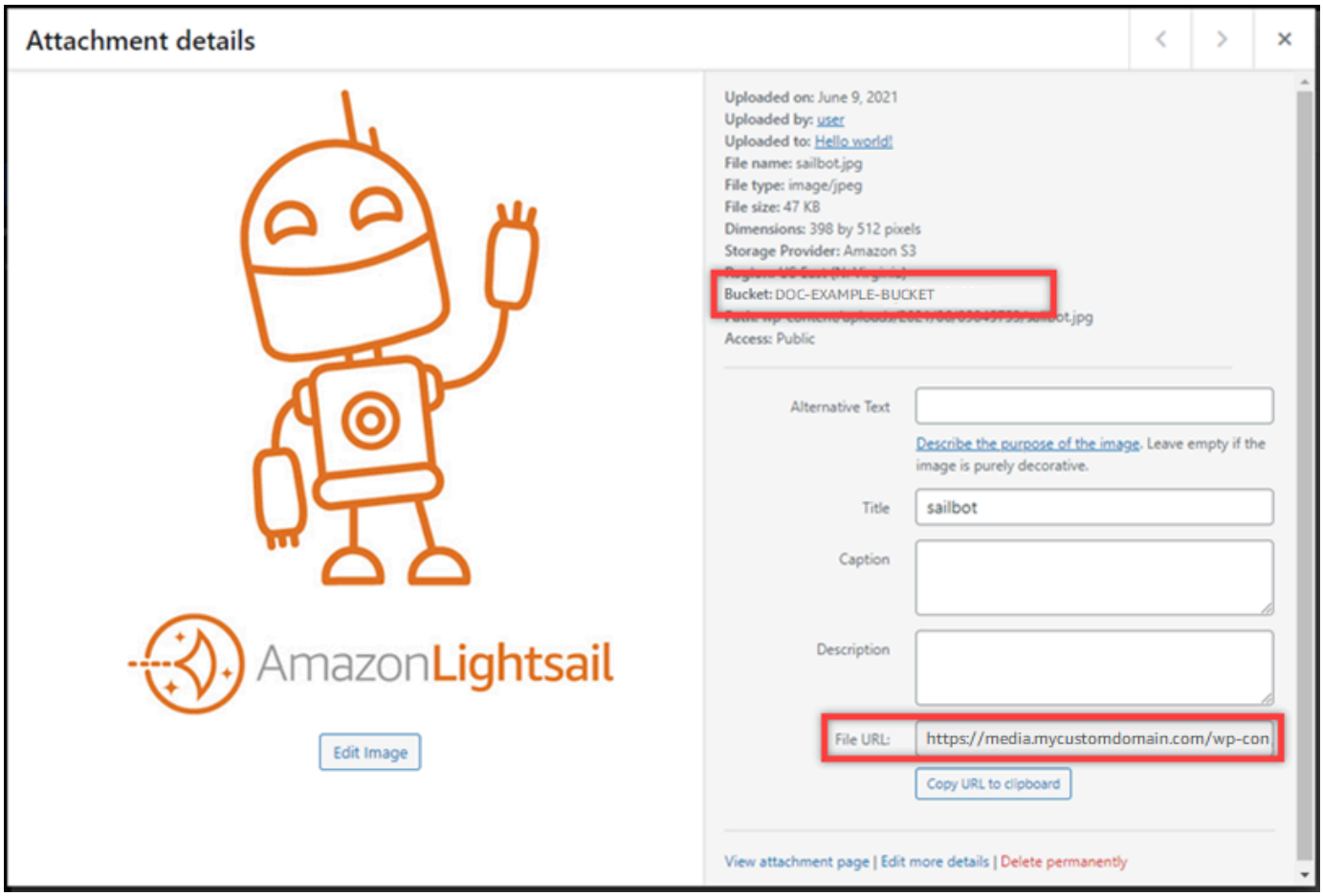
4. Wenn die Datei hochgeladen wurde, wählen Sie Bibliothek unter Medien im linken Navigationsmenü.



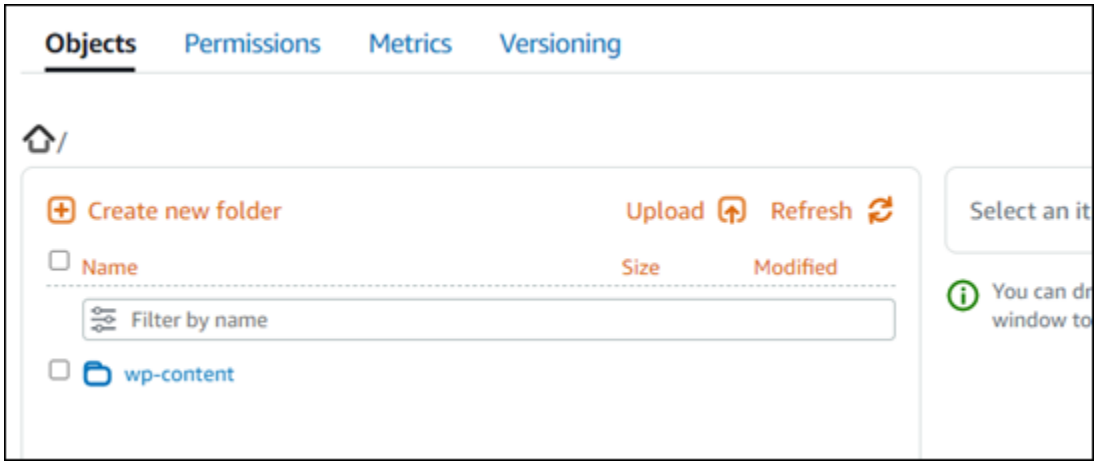
5. Wählen Sie die Datei aus, die Sie kürzlich hochgeladen haben.



6. Im Detailbereich der Datei wird der Name Ihres Buckets im FensterBucketfield. Die URL Ihrer Verteilung wird im Feld URL der Datei angezeigt.



7. Wenn Sie auf der Lightsail-Bucket-Verwaltungsseite zur Registerkarte Objekte wechseln, sollten Sie einen wp-content-Ordner sehen. Dieser Ordner wird durch das Offload Media Lite-Plugin erstellt und wird verwendet, um Ihre hochgeladenen Mediendateien zu speichern.



Verwalten von Buckets und Objekten

Dies sind die allgemeinen Schritte zur Verwaltung Ihres Lightsail-Objektspeicher-Buckets:

1. Erfahren Sie mehr über Objekte und Buckets im Amazon Lightsail-Objektspeicherdienst. Weitere Informationen finden Sie unter Objektspeicher in Amazon Lightsail.
2. Erfahren Sie mehr über die Namen, die Sie Ihren Buckets in Amazon Lightsail geben können. Weitere Informationen finden Sie unter Regeln für die Bucket-Benennung in Amazon Lightsail.
3. Beginnen Sie mit dem Lightsail-Objektspeicherdienst, indem Sie einen Bucket erstellen. Weitere Informationen finden Sie unter Erstellen von Buckets in Amazon Lightsail.
4. Erfahren Sie mehr über bewährte Sicherheitsmethoden für Buckets und die Zugriffsberechtigungen, die Sie für Ihren Bucket konfigurieren können. Sie können alle Objekte in Ihrem Bucket öffentlich oder privat machen, oder Sie können einzelne Objekte öffentlich machen. Sie können auch Zugriff auf Ihren Bucket gewähren, indem Sie Zugriffsschlüssel erstellen, Instances zu Ihrem Bucket hinzufügen und Zugriff auf andere AWS-Konten gewähren. Weitere Informationen finden Sie unter Bewährte Methoden für die Sicherheit von Amazon Lightsail-Objektspeichern und Grundlegendes zu Bucket-Berechtigungen in Amazon Lightsail.

   Nachdem Sie sich mit den Zugriffsberechtigungen für Buckets vertraut gemacht haben, lesen Sie in den folgenden Anleitungen nach, wie Sie Zugriff auf Ihren Bucket gewähren können:

   - Blockieren des öffentlichen Zugriffs für Buckets in Amazon Lightsail
   - Konfigurieren von Bucket-Zugriffsberechtigungen in Amazon Lightsail

- Konfigurieren von Zugriffsberechtigungen für einzelne Objekte in einem Bucket in Amazon Lightsail
- Erstellen von Zugriffsschlüsseln für einen Bucket in Amazon Lightsail
- Konfigurieren des Ressourcenzugriffs für einen Bucket in Amazon Lightsail
- Konfigurieren des kontoübergreifenden Zugriffs für einen Bucket in Amazon Lightsail

5. Erfahren Sie, wie Sie die Zugriffsprotokollierung für Ihren Bucket aktivieren und wie Sie mithilfe von Zugriffsprotokollen die Sicherheit Ihres Buckets überprüfen können. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Zugriffsprotokollierung für Buckets im Amazon Lightsail-Objektspeicherdienst
   - Zugriffsprotokollformat für einen Bucket im Amazon Lightsail-Objektspeicherdienst
   - Aktivieren der Zugriffsprotokollierung für einen Bucket im Amazon Lightsail-Objektspeicherdienst
   - Verwenden von Zugriffsprotokollen für einen Bucket in Amazon Lightsail zum Identifizieren von Anforderungen
6. Erstellen Sie eine IAM-Richtlinie, die einem Benutzer die Möglichkeit gibt, einen Bucket in Lightsail zu verwalten. Weitere Informationen finden Sie unter IAM-Richtlinie zum Verwalten von Buckets in Amazon Lightsail.
7. Erfahren Sie, wie Objekte in Ihrem Bucket beschriftet und identifiziert werden. Weitere Informationen finden Sie unter Grundlegendes zu Objektschlüsselnamen in Amazon Lightsail.
8. Erfahren Sie, wie Sie Dateien hochladen und Objekte in Ihren Buckets verwalten. Weitere Informationen finden Sie in den folgenden Anleitungen.
   - Hochladen von Dateien in einen Bucket in Amazon Lightsail
   - Hochladen von Dateien in einen Bucket in Amazon Lightsail mit mehrteiligem Upload
   - Anzeigen von Objekten in einem Bucket in Amazon Lightsail
   - Kopieren oder Verschieben von Objekten in einem Bucket in Amazon Lightsail
   - Herunterladen von Objekten aus einem Bucket in Amazon Lightsail
   - Filtern von Objekten in einem Bucket in Amazon Lightsail
   - Markieren von Objekten in einem Bucket in Amazon Lightsail
   - Löschen von Objekten in einem Bucket in Amazon Lightsail
9. Aktivieren Sie Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Bucket zu speichern, abzurufen oder wiederherzustellen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen des Objekt-Versionings in einem Bucket in Amazon Lightsail.

10. Nachdem Sie die Objekt-Versionsverwaltung aktiviert haben, können Sie frühere Versionen von Objekten in Ihrem Bucket wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen früherer Versionen von Objekten in einem Bucket in Amazon Lightsail.
11. Überwachen Sie die Auslastung Ihres Buckets. Weitere Informationen finden Sie unter Anzeigen von Metriken für Ihren Bucket in Amazon Lightsail.
12. Konfigurieren Sie einen Alarm für Bucket-Metriken, sodass Sie benachrichtigt werden, wenn die Auslastung Ihres Buckets einen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Erstellen von Bucket-Metrikalarmen in Amazon Lightsail.
13. Ändern Sie den Speicherplan Ihres Buckets, wenn der Speicherplatz und die Netzwerkübertragung knapp werden. Weitere Informationen finden Sie unter Ändern des Plans Ihres Buckets in Amazon Lightsail.
14. Erfahren Sie, wie Sie Ihren Bucket mit anderen Ressourcen verbinden. Weitere Informationen finden Sie in den folgenden Tutorials.
    - Tutorial: Verbinden einer WordPress Instance mit einem Amazon Lightsail-Bucket
    - Tutorial: Verwenden eines Amazon Lightsail-Buckets mit einer Netzwerkverteilung für die Bereitstellung von Inhalten in Lightsail
15. Löschen Sie Ihren Bucket, wenn Sie ihn nicht mehr verwenden. Weitere Informationen finden Sie unter Löschen von Buckets in Amazon Lightsail.

Verwenden von Lightsail mit anderen - AWS Services

Amazon Lightsail verwendet eine gezielte Reihe von AWS Services wie Amazon EC2 und , AWS Identity and Access Management um den Einstieg zu erleichtern. Sie sind jedoch nicht auf diese Services beschränkt!

Sie können Lightsail-Ressourcen über Amazon VPC Peering in andere - AWS Services integrieren. Weitere Informationen zur Einrichtung von VPC-Peering.

Folgen Sie den folgenden Links, um mehr über andere - AWS Services zu erfahren.

Virtuelle Maschinen (virtuelle private Server)

Amazon EC2

> Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webservice, der größenveränderbare Datenverarbeitungskapazität in der Cloud bereitstellt. Er ist darauf ausgelegt, webweites Cloud Computing für Entwickler zu vereinfachen.

Mit Amazon EC2 können Sie Kapazität mit minimalem Aufwand abrufen und konfigurieren. Er ermöglicht Ihnen die vollständige Kontrolle über Ihre Datenverarbeitungsressourcen sowie die Ausführung in der bewährten Datenverarbeitungsumgebung von Amazon. Amazon EC2 verkürzt die Zeit, die zum Abrufen und Starten neuer Server-Instances erforderlich ist, auf wenige Minuten, so dass Sie die Kapazität schnell nach oben oder unten skalieren können, wenn sich Ihre Datenverarbeitungsanforderungen ändern. Amazon EC2 verändert die Wirtschaftlichkeit der Datenverarbeitung, indem es Ihnen ermöglicht, nur für die tatsächlich genutzte Kapazität zu bezahlen. Amazon EC2 stellt Entwicklern Tools zur Verfügung, mit denen sie ausfallsichere Anwendungen erstellen und sich von den üblichen Ausfallszenarien isolieren können.

Weitere Informationen über Amazon EC2.

Amazon VPC

Mit Amazon Virtual Private Cloud (Amazon VPC) können Sie einen logisch isolierten Abschnitt der AWS -Cloud bereitstellen, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können. Sie haben die vollständige Kontrolle über Ihre virtuelle Netzwerkumgebung, u. a. bei der Auswahl Ihres eigenen IP-Adressbereichs, dem Erstellen von Subnetzen und der Konfiguration von Routing-Tabellen und Netzwerk-Gateways.

Die Netzwerkkonfiguration für Ihre Amazon VPC kann auf einfache Weise angepasst werden. Sie können beispielsweise ein öffentlich zugängliches Subnetz mit Zugriff auf das Internet für Ihre Webserver einrichten und Ihre Backend-Systeme, z. B. Datenbanken oder Anwendungsserver, in einem privaten Subnetz ohne Internetzugang betreiben. Sie können mehrere Sicherheitsebenen einrichten, darunter Sicherheitsgruppen und Netzwerk-Zugriffskontrolllisten (ACLs), die den Zugriff auf Amazon-EC2-Instances in den einzelnen Subnetzen steuern.

Zudem können Sie eine Hardware-VPN-Verbindung (Virtual Private Network) zwischen dem Rechenzentrum Ihres Unternehmens und Ihrer VPC erstellen und die AWS Cloud als Erweiterung für das Rechenzentrum Ihres Unternehmens einsetzen.

Weitere Informationen über Amazon VPC.

Serverloses Computing

AWS Lambda

AWS Lambda Mit können Sie Code ausführen, ohne Server bereitstellen oder verwalten zu müssen. Sie zahlen nur für die genutzte Rechenzeit. Wenn Ihr Code nicht ausgeführt wird, wird auch nichts berechnet. Mit Lambda können Sie Code für nahezu jede Anwendungsart oder jeden

Backend-Service ausführen und zwar ohne Administration. Sie laden einfach Ihren Code hoch und Lambda kümmert sich darum, dass Ihr Code mit hoher Verfügbarkeit ausgeführt und skaliert wird. Sie können Ihren Code so einrichten, dass er automatisch von anderen AWS-Services ausgelöst wird, oder ihn indirekt von einer beliebigen Web- oder Mobil-App aufrufen.

Weitere Informationen über AWS Lambda.

Amazon API Gateway

Amazon API Gateway ist ein vollständig verwalteter Service, der es Entwicklern leicht macht, APIs in beliebigem Umfang zu erstellen, zu veröffentlichen, zu pflegen, zu überwachen und zu sichern. Mit ein paar Klicks in der AWS Management Console können Sie ein API erstellen, das als "Haupteingang" für Anwendungen dient, um auf Daten, Geschäftslogik oder Funktionen von Ihren Backend-Services zuzugreifen. Dazu gehören Workloads, die auf Amazon EC2 laufen, Code, der auf Lambda ausgeführt wird oder beliebige Webanwendungen. Amazon API Gateway handhabt sämtliche Aufgaben im Zusammenhang mit der Annahme und Verarbeitung von Hunderttausenden gleichzeitiger API-Aufrufe. Dazu gehören Datenverkehrsmanagement, Autorisierung und Zugriffskontrolle, Überwachung und API-Versionsmanagement. Für Amazon API Gateway fallen weder Mindestgebühren noch Vorabkosten an. Sie zahlen nur für die API-Aufrufe, die Sie erhalten, und nach außen übertragenen Daten.

Erfahren Sie mehr über Amazon API Gateway.

Datenbanken

Amazon DynamoDB

Amazon DynamoDB ist ein schneller und flexibler NoSQL-Datenbank-Service für alle Anwendungen, die für beliebig große Datenmengen eine konsistente, einstellige Latenz im Millisekundenbereich benötigen. Es handelt sich um eine vollständig verwaltete Cloud-Datenbank, die sowohl Dokument- als auch Schlüssel-Wert-Speichermodelle unterstützt. Aufgrund seines flexiblen Datenmodells und seiner zuverlässigen Leistung ist DynamoDB hervorragend geeignet für Spiele, Web-, Ad-Tech-, IoT-, mobile und andere Anwendungen.

Erfahren Sie mehr über DynamoDB.

Amazon RDS

Amazon Relational Database Service (Amazon RDS) macht es einfach, eine relationale Datenbank in der Cloud einzurichten, zu betreiben und zu skalieren. Er bietet eine kosteneffiziente

und anpassbare Kapazität und verwaltet gleichzeitig zeitaufwändige Aufgaben der Datenbankverwaltung, so dass Sie sich auf Ihre Anwendungen und Ihr Geschäft konzentrieren können. Amazon RDS bietet sechs gängige Datenbank-Engines zur Auswahl. Dazu gehören unter anderem: Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle und Microsoft SQL Server.

Weitere Informationen über Amazon RDS.

Amazon Aurora

Amazon Aurora ist eine MySQL-kompatible relationale Datenbank-Engine , die die Geschwindigkeit und Verfügbarkeit einer hochwertigen kommerziellen Datenbank mit der Wirtschaftlichkeit einer Open-Source-Datenbank verbindet. Aurora bietet eine bis zu fünf Mal bessere Performance als MySQL mit der Sicherheit, Verfügbarkeit und Zuverlässigkeit einer kommerziellen Datenbank zu einem Zehntel der Kosten.

Weitere Informationen über Amazon Aurora.

Load Balancers

Elastic Load Balancing

Elastic Load Balancing verteilt den eingehenden Anwendungsverkehr automatisch auf mehrere Amazon-EC2-Instances. Somit kann Fehlertoleranz in Ihren Anwendungen erreicht werden: Die für die Weiterleitung von Anwendungsverkehr notwendige Lastverteilungskapazität wird nahtlos an den Anwendungsverkehr angepasst.

Elastic Load Balancing unterstützt zwei verschiedene Load Balancer-Typen. Beide bieten höchste Verfügbarkeit, automatische Skalierung und robuste Sicherheit. Dazu gehören der Classic Load Balancer, der den Datenverkehr entweder auf der Grundlage von Informationen auf Anwendungs- oder auf Netzwerkebene leitet, und der Application Load Balancer, der den Datenverkehr auf der Grundlage erweiterter Informationen auf Anwendungsebene leitet, welche den Inhalt der Anfrage umfassen. Der Classic Load Balancer eignet sich ideal für die einfache Lastverteilung von Datenverkehr auf mehrere Amazon-EC2-Instances. Der Application Load Balancer eignet sich ideal für Anwendungen, die erweiterte Routing-Funktionen benötigen, Micro-Services und Container-basierte Architekturen. Der Application Load Balancer bietet die Möglichkeit, Netzwerkverkehr zu mehreren Services zu routen oder eine Lastverteilung auf mehreren Ports derselben Amazon-EC2-Instance durchzuführen.

Erfahren Sie mehr über Elastic Load Balancing.

Application Load Balancer

Ein Application Load Balancer ist eine Lastverteilungsoption für den Elastic-Load-Balancing-Service, der auf der Anwendungsschicht arbeitet und ermöglicht, dass Sie auf dem Inhalt basierende Weiterleitungsregeln über mehrere Services oder Container definieren, die auf einer oder mehreren Amazon-EC2-Instances ausgeführt werden.

Erfahren Sie mehr über Application Load Balancer.

Big Data

Amazon-Kinesis-Services

Amazon-Kinesis-Services erleichtern Ihnen die Arbeit mit Echtzeit-Streaming-Daten in der AWS-Cloud. Amazon Kinesis Services umfassen Folgendes: Amazon Data Firehose zum einfachen Laden riesiger Mengen von Streaming-Daten in AWS, Amazon Managed Service für Apache Flink zum Analysieren von Streaming-Daten mit Standard-SQL und Amazon Kinesis Data Streams zum Erstellen eigener benutzerdefinierter Anwendungen, die Streaming-Daten verarbeiten oder analysieren.

Erfahren Sie mehr über Amazon-Kinesis-Services.

Amazon EMR

Amazon EMR bietet ein verwaltetes Hadoop-Framework, mit dem Sie große Datenmengen einfach, schnell und kostengünstig auf dynamisch skalierbaren Amazon-EC2-Instances verarbeiten können. Sie können auch andere beliebte verteilte Frameworks wie Apache Spark, HBase, Presto und Flink in Amazon EMR ausführen und mit Daten in anderen AWS-Datenspeichern wie Amazon S3 und DynamoDB interagieren.

Amazon EMR verarbeitet sicher und zuverlässig eine breite Palette von Big Data-Anwendungsfällen. Hierzu zählen unter anderem Protokollanalysen, Web-Indizierungen, Datentransformationen (ETL), Machine Learning, Finanzanalysen, wissenschaftliche Simulationen und Bioinformatik.

Weitere Informationen über Amazon EMR.

Amazon Redshift

Amazon Redshift ist ein schneller, vollständig verwalteter Data Warehouse-Service für Datenmengen im Petabyte-Bereich, mit dem Sie im Zusammenspiel mit Ihren vorhandenen Business-Intelligence-Tools alle Ihre Daten einfach und wirtschaftlich analysieren können.

Weitere Informationen über Amazon Redshift.

Speicher

Amazon Simple Storage Service (Amazon S3)

Amazon S3 bietet Entwicklern und IT-Teams sicheren, beständigen und hochgradig skalierbaren Cloud-Speicher. Amazon S3 ist easy-to-use Objektspeicher mit einer einfachen Webservice-Schnittstelle zum Speichern und Abrufen beliebiger Datenmengen von überall im Internet. Mit Amazon S3 zahlen Sie nur für den Speicherplatz, den Sie tatsächlich nutzen. Es fallen weder Mindestgebühren noch Einrichtungskosten an.

Amazon S3 bietet viele verschiedene Speicherklassen, die auf die unterschiedlichen Anwendungsfälle zugeschnitten sind: Amazon S3 Standard Standard zur allgemeinen Speicherung häufig verwendeter Daten, Amazon S3 Standard – Infrequent Access (Standard-IA) für langlebige, aber weniger häufig benutzte Daten, und S3 Glacier als Langzeitarchiv. Amazon S3 bietet außerdem konfigurierbare Lebenszyklusrichtlinien für die Verwaltung Ihrer Daten während ihres gesamten Lebenszyklus. Sobald eine Richtlinie festgelegt wurde, werden Ihre Daten automatisch in die am besten geeignete Speicherklasse migriert, ohne irgendwelche Änderungen an Ihren Anwendungen vorzunehmen.

Amazon S3 kann eigenständig oder zusammen mit anderen AWS-Services wie Amazon EC2 und IAM verwendet werden, ebenso wie mit Cloud-Datenmigrationsservices und Gateways für eine initiale oder stetige Datenerfassung. Amazon S3; bietet einen kosteneffektiven Objektspeicher für eine Vielzahl an Anwendungsfällen, wie beispielsweise Sicherung und Wiederherstellung, Nearline-Archivierung, Big-Data-Analytik, Notfallwiederherstellung, Cloud-Anwendungen und Inhaltsverteilung.

Weitere Informationen über Amazon S3.

Amazon Elastic Block Store (Amazon EBS)

Amazon EBS bietet Volumes für persistente Speicherung auf Blockebene zur Verwendung mit Amazon-EC2-Instances in der AWS Cloud. Jedes Amazon-EBS-Volume wird in seiner Availability Zone automatisch repliziert, um Schutz bei Ausfall von Komponenten zu bieten, was für hohe Verfügbarkeit und Beständigkeit sorgt. Amazon-EBS-Volumes bieten die einheitliche Leistung und niedrige Latenz, die Sie zum Bewältigen Ihrer Workloads benötigen. Mit Amazon EBS können Sie die genutzten Kapazitäten innerhalb von wenigen Minuten auf- und abskalieren. Die geringen Kosten entstehen hierbei nur für die Ressourcen, die Sie bereitstellen.

Weitere Informationen über Amazon EBS.

Überwachung und Alarme

Amazon CloudWatch

Amazon CloudWatch ist ein Überwachungsservice für AWS Cloud-Ressourcen und die Anwendungen, die Sie auf AWS ausführen. Sie können verwenden, CloudWatch um Metriken zu erfassen und zu verfolgen, Protokolldateien zu sammeln und zu überwachen, Alarme festzulegen und automatisch auf Änderungen in Ihren AWS-Ressourcen zu reagieren. CloudWatch kann AWS-Ressourcen wie Amazon EC2-Instances, Amazon DynamoDB-Tabellen und Amazon RDS-DB-Instances sowie benutzerdefinierte Metriken überwachen, die von Ihren Anwendungen und Services generiert werden, und auf alle Protokolldateien, die Ihre Anwendungen generieren. Sie können verwenden CloudWatch , um einen systemweiten Einblick in die Ressourcenauslastung, die Anwendungsleistung und den Betriebszustand zu erhalten. Auf der Grundlage dieser Einsichten können Sie reagieren und so zu einer störungsfreien Ausführung Ihrer Anwendung beitragen.

Weitere Informationen über Amazon CloudWatch.

Bereitstellen von Anwendungen

AWS Elastic Beanstalk

AWS Elastic Beanstalk ist ein - easy-to-use Service für die Bereitstellung und Skalierung von Webanwendungen und -Services, die mit Java, .NET, PHP, Node.js, Python, Ruby, Go und Docker auf vertrauten Servern wie Apache, Nginx, Passenger und IIS entwickelt wurden.

Sie laden Ihren Code einfach hoch und Elastic Beanstalk übernimmt automatisch die Bereitstellung, von der Kapazitätsbereitstellung, Load-Balancing und Auto Scaling bis zur Statusüberwachung der Anwendung. Gleichzeitig erhalten Sie mit Elastic Beanstalk vollständige Kontrolle über die AWS-Ressourcen hinter Ihrer Anwendung und können jederzeit auf die zugrunde liegenden Ressourcen zugreifen.

Erfahren Sie mehr über Elastic Beanstalk.

Anwendungscontainer

Amazon Elastic Container Service (Amazon ECS)

Amazon ECS ist ein hoch skalierbarer und äußerst leistungsfähiger Container-Management-Service, der Docker-Container unterstützt und es Ihnen erlaubt, Anwendungen auf einem verwalteten Cluster von Amazon-EC2-Instances auf einfache Art zu betreiben. Amazon ECS erspart Ihnen die Installation, den Betrieb und die Skalierung Ihrer eigenen Cluster-Management-Infrastruktur. Mit einfachen API-Aufrufen können Sie Docker-fähige Anwendungen starten und stoppen, den kompletten Status Ihres Clusters abfragen und auf viele bekannte Funktionen wie Sicherheitsgruppen, Elastic-Load-Balancing, Amazon-EBS-Volumes und IAM-Rollen zugreifen. Mit Amazon ECS können Sie die Platzierung von Containern in Ihrem Cluster entsprechend Ihrem Ressourcenbedarf und Ihren Verfügbarkeitserfordernissen planen. Außerdem können Sie Ihren eigenen Scheduler oder Scheduler von Drittanbietern für geschäfts- oder anwendungsspezifische Anforderungen integrieren.

Weitere Informationen über Amazon ECS.

Sicherheit und Benutzeranmeldung

AWS Identity and Access Management (IAM)

Mit IAM können Sie den Zugriff auf AWS-Services und -Ressourcen für Ihre Benutzer sicher steuern. Mithilfe von IAM können Sie AWS-Benutzer und -Gruppen anlegen und verwalten und mittels Berechtigungen ihren Zugriff auf AWS-Ressourcen zulassen oder verweigern.

Weitere Informationen über IAM.

Amazon Cognito-Benutzerpools

Mit Amazon Cognito können Sie Benutzerregistrierung und -anmeldung in Ihren Mobil- und Webanwendungen auf einfache Weise hinzufügen. Mit Amazon Cognito haben Sie die Möglichkeit, Benutzer über Social-Identity-Anbieter wie Facebook, Twitter oder Amazon, über SAML-Identitätslösungen oder über Ihr eigenes Identitätssystem zu authentifizieren. Zusätzlich können Sie mit Amazon Cognito Daten lokal auf den Geräten der Benutzer speichern. So funktionieren Ihre Anwendungen auch dann, wenn die Geräte offline sind. Die Daten können auf den Geräten der Benutzer synchronisiert werden. Die App-Umgebung bleibt daher immer gleich – egal, auf welchem Gerät die App genutzt wird.

Mit Amazon Cognito können Sie sich auf das Entwickeln herausragender Anwendungserlebnisse konzentrieren und müssen sich keine Gedanken mehr über das Erstellen, Sichern und Skalieren einer Lösung für die Benutzerverwaltung, -authentifizierung und die geräteübergreifende Synchronisierung machen.

Weitere Informationen über Amazon Cognito.

Versionsverwaltung und Verwaltung des Anwendungslebenszyklus

AWS CodeCommit

AWS CodeCommit ist ein vollständig verwalteter Quellcodeverwaltungsservice, der es Unternehmen vereinfacht, sichere und hochgradig skalierbare private Git-Repositorys zu hosten. AWS CodeCommit macht es überflüssig, Ihr eigenes Quellcodeverwaltungssystem zu betreiben oder sich Gedanken über die Skalierung seiner Infrastruktur zu machen. Sie können verwenden AWS CodeCommit , um alles, vom Quellcode bis zu Binärdateien, sicher zu speichern, und es funktioniert nahtlos mit Ihren vorhandenen Git-Tools.

Weitere Informationen über AWS CodeCommit.

Warteschlangen und Messaging

Amazon SQS

Amazon Simple Queue Service (Amazon SQS) ist ein schneller, zuverlässiger, skalierbarer, vollständig verwalteter Service für die Nachrichten-Warteschlangen-Service. Amazon SQS ermöglicht eine einfache und wirtschaftliche Entkopplung der Komponenten einer Cloud-Anwendung. Mit Amazon SQS können Sie beliebige Datenvolumen übertragen, ohne dass Nachrichten verloren gehen oder andere Services stets verfügbar sein müssen. Amazon SQS umfasst Standardwarteschlangen mit hohem Durchsatz und hoher at-least-once Verarbeitung sowie FIFO-Warteschlangen, die eine FIFO-Bereitstellung (First-In, First-Out) und eine exakt einmalige Verarbeitung ermöglichen.

Mit Amazon SQS können Sie den administrativen Aufwand von Betrieb und Skalierung hoch verfügbarer Cluster für die Nachrichtenübermittlung auslagern und zahlen nur einen geringen Preis für die tatsächlich in Anspruch genommenen Ressourcen.

Weitere Informationen über Amazon SQS.

Amazon SNS

Amazon Simple Notification Service (Amazon SNS) ist ein schneller, flexibler und vollständig verwalteter Push-Benachrichtigungsdienst, über den Sie einzelne Nachrichten oder Rundsendungen an eine große Zahl von Empfängern senden können. Amazon SNS ermöglicht das einfache und kostengünstige Senden von Push-Benachrichtigungen an Benutzer mobiler Geräte, E-Mail-Empfänger und sogar an andere verteilte Services.

Mit Amazon SNS können Sie Benachrichtigungen an den Apple Push Notification Service (APNS), das Google Cloud Messaging (GCM), Fire OS- und Windows-Geräte sowie an Android-Geräte in China mit Baidu Cloud Push senden. Mit Amazon SNS können Sie weltweit SMS-Mitteilungen an Nutzer von mobilen Geräten senden.

Über diese Endpunkte hinaus kann Amazon SNS auch Nachrichten an Amazon SQS, AWS Lambda -Funktionen und jegliche HTTP-Endpunkte senden.

Weitere Informationen über Amazon SNS.

Amazon SES

Amazon Simple Email Service (Amazon SES) ist ein kosteneffektiver E-Mail-Service, der auf der zuverlässigen und skalierbaren, von Amazon.com zur eigenen Nutzung entwickelten Infrastruktur basiert. Mit Amazon SES können Sie E-Mails ohne Vertragsbindung senden und empfangen. Die Zahlung ist leistungsbasiert und fällt nur für Ihre tatsächliche Nutzung an.

Weitere Informationen über Amazon SES.

Workflow

Amazon Simple Workflow Service (Amazon SWF)

Amazon SWF ist ein vollständig verwalteter Service, mit dem Entwickler Hintergrundjobs, die parallele oder sequenzielle Schritte umfassen, programmieren, ausführen und skalieren können. Stellen Sie sich Amazon SWF wie einen vollständig verwalteten Status-Tracker und Aufgabenkoordinator in der Cloud vor.

Wenn die Schritte Ihrer Anwendung mehr als 500 Millisekunden dauern, müssen Sie den Stand der Verarbeitung verfolgen und bei einem Fehlschlag eine Wiederherstellung oder einen neuen Versuch durchführen. Amazon SWF kann Ihnen helfen.

Weitere Informationen über Amazon SWF.

Streaming von Anwendungen

Amazon AppStream

Mit Amazon AppStream können Sie Ihre Windows-Anwendungen auf jedem Gerät bereitstellen.

Mit Amazon AppStream können Sie Ihre vorhandenen Windows-Anwendungen aus der Cloud streamen und mehr Benutzer auf mehr Geräten erreichen, ohne Codeänderungen vorzunehmen. Mit Amazon wird AppStreamIhre Anwendung in der - AWS Infrastruktur bereitgestellt und gerendert, und die Ausgabe wird an Massengeräte wie PCs, Tablets und Mobiltelefone gestreamt. Da Ihre Anwendung in der Cloud ausgeführt wird, kann sie zum Bewältigen umfangreicher Rechen- und Speicheranforderungen skaliert werden, und zwar unabhängig von den Geräten, die Ihre Kunden nutzen. Amazon AppStream bietet ein SDK zum Streamen Ihrer Anwendung aus der Cloud. Sie können Ihre eigenen benutzerdefinierten Clients, Abonnements, Identitäts- und Speicherlösungen in Amazon integrieren, AppStream um eine benutzerdefinierte Streaming-Lösung zu entwickeln, die den Anforderungen Ihres Unternehmens entspricht.

Weitere Informationen über Amazon AppStream.

Lightsail-Ressourcen erstellen mit AWS CloudFormation

Amazon Lightsail ist in AWS CloudFormation integriert, ein Service, der Ihnen hilft, Ihre AWS-Ressourcen zu modellieren und einzurichten, damit Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen können. Sie erstellen eine Vorlage, in der alle gewünschten AWS-Ressourcen beschrieben werden (wie z. B. Instances und Festplatten) und AWS CloudFormation übernimmt dann die Bereitstellung und Konfiguration dieser Ressourcen für Sie.

Wenn Sie AWS CloudFormation verwenden, können Sie Ihre Vorlage wiederverwenden, um Ihre Lightsail-Ressourcen einheitlich und wiederholt einzurichten. Sie beschreiben Ihre Ressourcen dann einmal und können die gleichen Ressourcen dann in mehreren AWS-Konten-Konten und -Regionen immer wieder bereitstellen.

Lightsail- und AWS CloudFormation-Vorlagen

Um Ressourcen für Lightsail und verwandte Dienstleistungen bereitzustellen und zu konfigurieren, müssen Sie AWS CloudFormation-Vorlagen kennen und verstehen. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS

CloudFormation-Stacks bereitstellen möchten. Wenn Sie noch keine Erfahrungen mit JSON oder YAML haben, können Sie AWS CloudFormation Designer verwenden, der den Einstieg in die Arbeit mit AWS CloudFormation-Vorlagen erleichtert. Weitere Informationen finden Sie unter Was ist AWS CloudFormation-Designer? im AWS CloudFormation-Benutzerhandbuch.

Lightsail unterstützt das Erstellen von Instances und Festplatten in AWS AWS CloudFormation. Weitere Informationen finden Sie unter Lightsail-Ressourcentypenreferenz im AWS CloudFormation-Benutzerhandbuch.

Weitere Informationen zu AWS CloudFormation

Weitere Informationen zu AWS CloudFormation finden Sie in den folgenden Ressourcen.

- AWS CloudFormation
- AWS CloudFormation-Benutzerhandbuch
- AWS CloudFormation API Referenz
- AWS CloudFormation-Benutzerhandbuch für die Befehlszeilenschnittstelle

AWS CloudFormation-Stacks für Lightsail

Amazon Lightsail verwendet AWS CloudFormation, um Amazon Elastic Compute Cloud (Amazon EC2)-Instances aus exportierten Snapshots zu erstellen. Ein CloudFormation-Stack wird erstellt, wenn Sie veranlassen, dass eine Amazon-EC2-Instance über die Lightsail-Konsole oder die Lightsail-API erstellt wird. Der Stack führt eine Reihe von Aktionen in Ihrem Amazon Web Services (AWS)-Konto durch, um alle zugehörigen Ressourcen für die Instance zu erstellen, wie z. B. die Amazon EC2-Instance aus einem Amazon Machine Image (AMI), das Elastic Block Store (EBS)-System-Volume aus einem EBS-Snapshot und die Sicherheitsgruppe für die Instance. Weitere Informationen zu AWS CloudFormation-Stacks finden Sie unter Arbeiten mit Stacks in der Dokumentation zu AWS CloudFormation.

Sie können auf die AWS CloudFormation-Stacks über die Lightsail-Konsole oder in der AWS CloudFormation-Konsole zugreifen. Diese Anleitung zeigt Ihnen, wie Sie auf beide zugreifen können.

> **Note**
>
> Der AWS CloudFormation-Stack, der zur Erstellung Ihrer Amazon EC2-Ressourcen verwendet wird, ist permanent mit Ihren Amazon-EC2-Ressourcen verknüpft. Wenn Sie den Stack löschen, werden alle zugehörigen Ressourcen automatisch gelöscht. Aus diesem

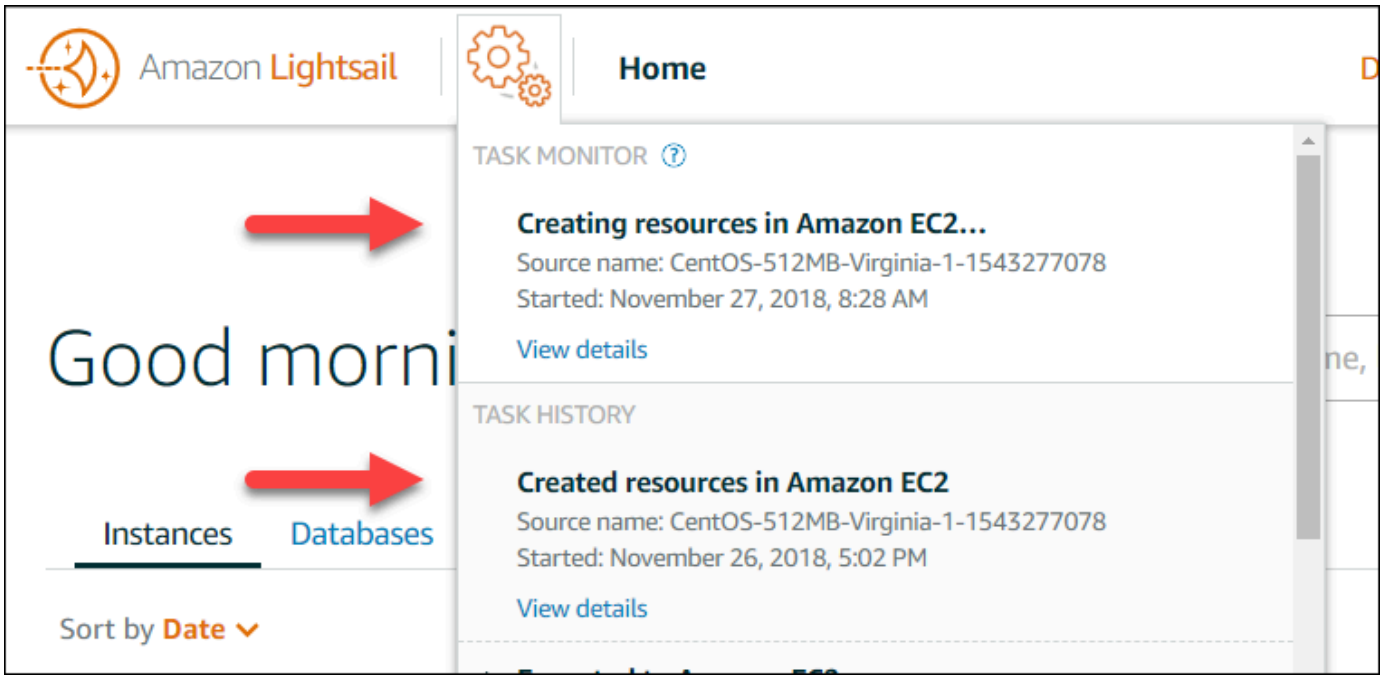
Grund sollten Sie keinen der von Lightsail erstellten AWS CloudFormation-Stacks löschen, sondern stattdessen Ihre Amazon-EC2-Ressourcen über die EC2-Konsole löschen.

Zugreifen auf die AWS CloudFormation-Stacks über die Lightsail-Konsole

Nachdem Sie sich entschieden haben, eine Instance in Amazon EC2 über die Lightsail-Konsole oder die Lightsail-API zu erstellen, wird ein AWS CloudFormation-Stack erstellt und sein Status über die Aufgabenüberwachung verfolgt. Weitere Informationen zur Aufgabenüberwachung finden Sie unter Aufgabenüberwachung.

So zeigen Sie Ihre AWS CloudFormation-Stacks in der Lightsail-Konsole an

1. Melden Sie sich an der Lightsail-Konsole an.
2. Wählen Sie im oberen Navigationsbereich die Aufgabenüberwachung aus.
3. Um auf einen CloudFormation-Stack für eine zuvor erstellte Amazon EC2-Instance zuzugreifen, wählen Sie View details (Details anzeigen) für eine mit Creating resources in Amazon EC2 (Ressourcen in Amazon EC2 erstellen) oder Created resources in Amazon EC2 (Ressourcen in Amazon EC2 erstellen) gekennzeichnete Aufgabe aus.

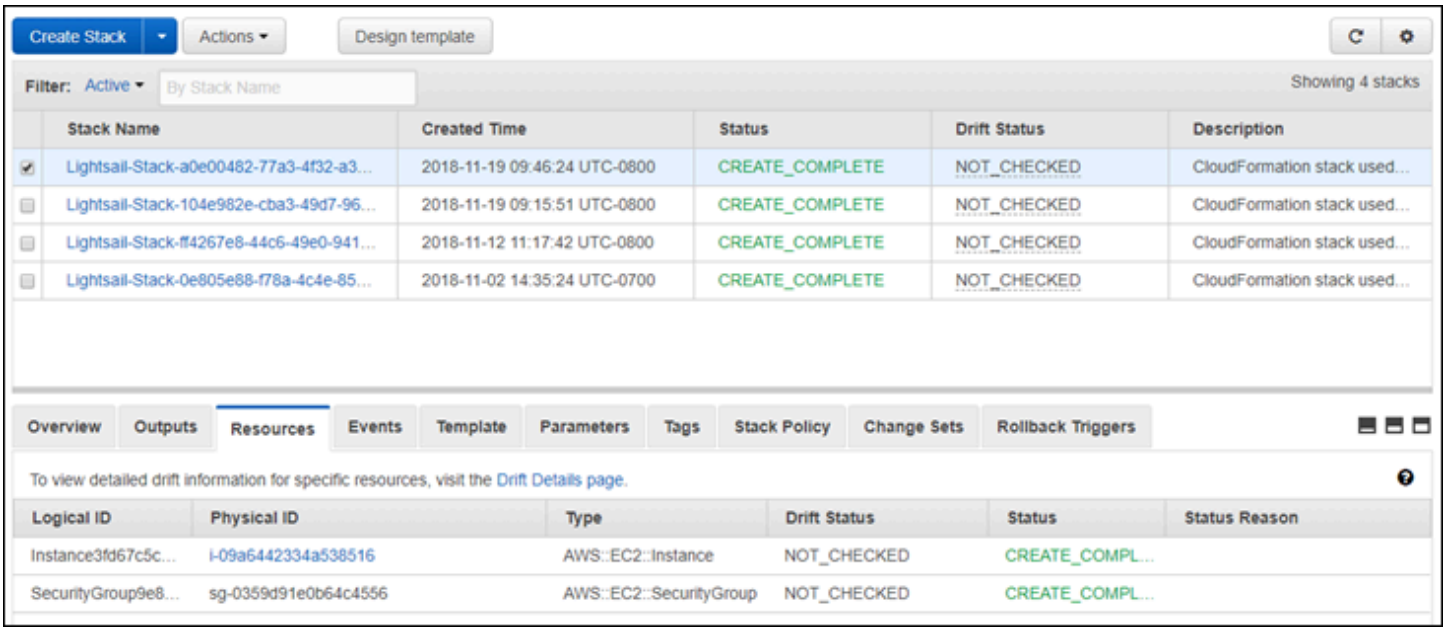


4. Die angezeigte Bestätigungsseite listet den CloudFormation-Stack für die Aufgabe auf. Wählen Sie den Stack-Namen aus, um die Stack-Details in der AWS CloudFormation-Konsole zu öffnen.

Zugreifen auf die Stacks über die AWS CloudFormation-Konsole

Sie können auf Ihre Stack-Details auch über die AWS CloudFormation-Konsole zugreifen. Die von Lightsail erstellten Stacks beginnen mit „Lightsail-stack“ und haben die Beschreibung „CloudFormation-Stack verwendet, um Amazon-EC2-Ressourcen zu erstellen“, wie im folgenden Screenshot gezeigt.

Stacks mit dem Status CREATE_IN_PROGRESS sind dabei, Amazon-EC2-Ressourcen aus Ihren exportierten Lightsail-Snapshots zu erstellen. Stacks mit dem Status CREATE_COMPLETED haben den Prozess der Erstellung von Amazon EC2-Ressourcen abgeschlossen. Um die von einem Stack erstellten Ressourcen anzuzeigen, aktivieren Sie das Kontrollkästchen neben dem Stack-Namen und wählen Sie dann die Registerkarte Resources (Ressourcen) aus.



Amazon Lightsail-Abrechnung

Die Abrechnung für Amazon Lightsail wird über Amazon Web Services (AWS)-Abrechnung abgehandelt. Um Ihre Lightsail-Rechnung anzuzeigen, wechseln Sie zumAWS Billing and Cost Management-Dashboard oder wählen Sie Billing (Fakturierung) in der oberen Navigationsleiste der Lightsail-Konsole aus. Weitere Informationen zu Preisen finden Sie auf der Seite Preise für Lightsail.

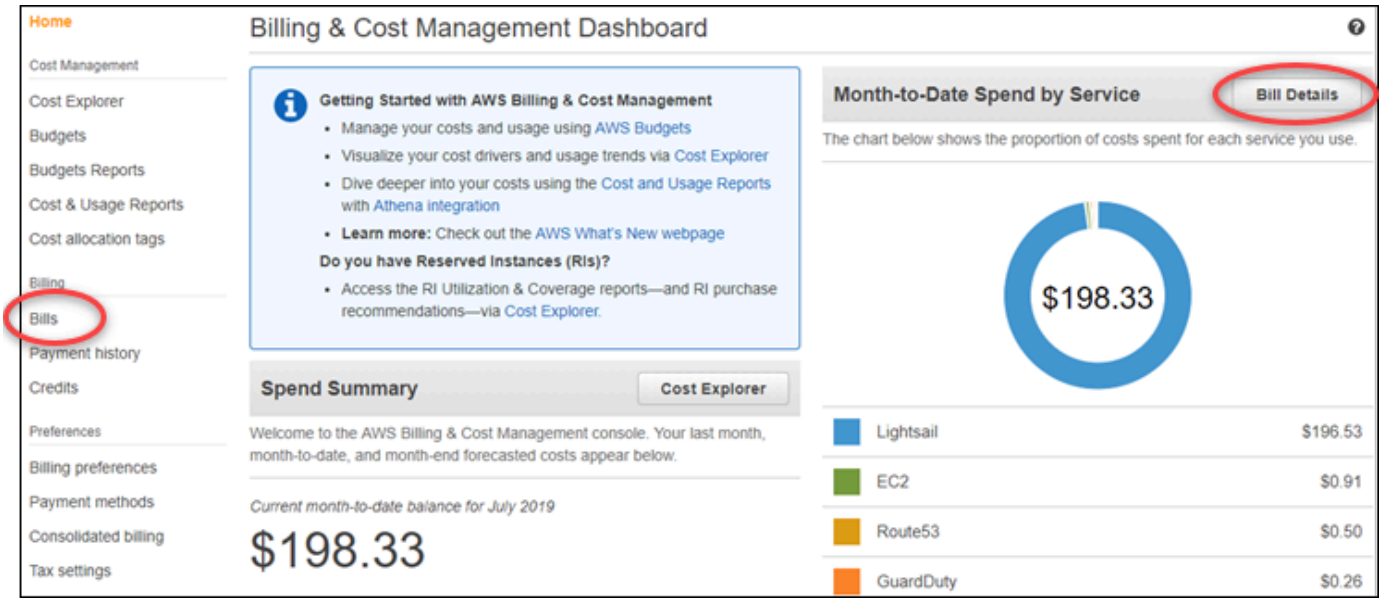
Anzeigen Ihrer detaillierten Lightsail-Rechnung

So zeigen Sie eine detaillierte Aufschlüsselung Ihrer monatlichen Lightsail-Rechnung an:

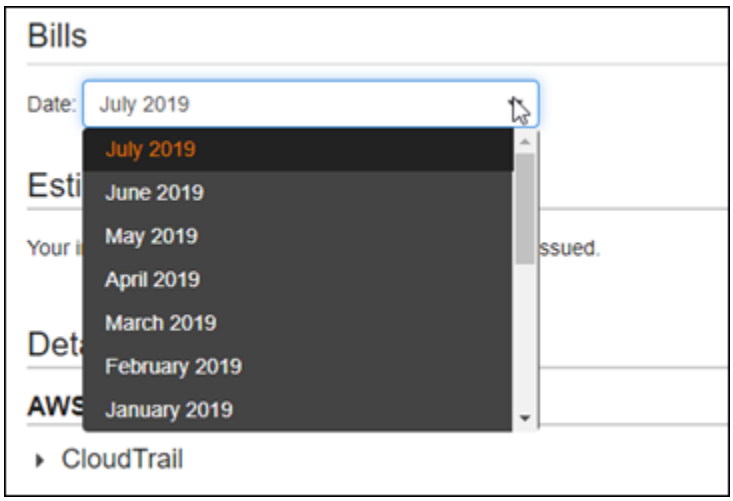
1. Melden Sie sich beim AWS Billing and Cost Management-Dashboardan.

   Auf der Startseite des Fakturierungs-Dashboards wird eine allgemeine Aufschlüsselung Ihrer Rechnung für den bisherigen Monat angezeigt.

2. Wählen Sie Bill Details (Rechnungsdetails) auf der Dashboard-Startseite oder Bills (Rechnungen) im linken Navigationsbereich aus, um eine detaillierte Version Ihrer monatlichen Rechnung anzuzeigen.



3. Wählen Sie das Dropdown-Menü Date (Datum) aus, um einen anderen Monat als den aktuellen Monat auszuwählen.



4. Scrollen Sie auf der Seite Bills (Rechnungen) nach unten und erweitern Sie den Eintrag Lightsail, um detaillierte Nutzungsinformationen für jede Region anzuzeigen.

Fakturierungsnutzungstypen

In der folgenden Liste werden die Nutzungstypen beschrieben, die in Ihren Lightsail-Fakturierungs- und -Nutzungsberichten angezeigt werden. Mithilfe dieser Nutzungstypen können Sie die Gebühren auf Ihrer monatlichen Rechnung für Lightsail-Ressourcen ermitteln.

> **Note**
>
> Beachten Sie für die folgenden Verwendungstypen, die einen Regionscode angeben, die Informationen im Abschnitt Regionscodes in Ihrer Rechnung in diesem Handbuch, um die entsprechende AWS-Region zu ermitteln.

- Amazon Lightsail Bundle: SizeGB: Der verwendete Linux- oder Unix-Instance-Plan (in Stunden). Die Größe (Size) definiert die Speicherspezifikation des verwendeten Instance-Plans. Wenn beispielsweise 4 GB Arbeitsspeicher angegeben sind, werden die abgerechneten Stunden für den Linux- oder Unix-Instance-Plan mit 20 USD/Monat angezeigt.
- Amazon LightsailBundle:SizeGB (Windows): Der verwendete Windows-Instance-Plan (in Stunden). Die Größe (Size) definiert die Speicherspezifikation des verwendeten Instance-Plans. Wenn beispielsweise 4 GB Arbeitsspeicher angegeben sind, werden die abgerechneten Stunden für den Windows-Instance-Plan mit 40 USD/Monat angezeigt.
- Amazon Lightsail RelationalDatabase: SizeGB: Die verwendeten Standarddatenbankpläne (in Stunden). Die Größe (Size) definiert die Speicherspezifikation des verwendeten Datenbankplans. Wenn beispielsweise 4 GB Arbeitsspeicher angegeben sind, werden die abgerechneten Stunden für den Standarddatenbankplan mit 60 USD/Monat angezeigt.
- Amazon Lightsail RelationalDatabase: SizeGB (hohe Verfügbarkeit): Die verwendeten Hochverfügbarkeits-Datenbankpläne (in Stunden). Die Größe (Size) definiert die Speicherspezifikation des verwendeten Datenbankplans. Wenn beispielsweise 4 GB Arbeitsspeicher angegeben sind, werden die abgerechneten Stunden für den Hochverfügbarkeits-Datenbankplan mit 120 USD/Monat angezeigt.
- Amazon Lightsail Region-DiskUsage: Die verwendete Menge Blockspeicherdatenträger (in Gigabyte pro Monat).
- Amazon Lightsail DNS-Queries: Die Anzahl der DNS-Abfragen für den Monat.
- Amazon Lightsail Load Balancer: Die Anzahl der verwendeten Load Balancer (in Stunden).
- Amazon Lightsail Region-SnapshotUsage: Die Menge der gespeicherten Snapshot-Daten (in Gigabyte pro Monat).
- Amazon Lightsail Region-UnusedStaticIP: Die Anzahl der nicht angefügten statischen IPs (in Stunden).
- Amazon Lightsail Region-TotalDataXfer-In-Bytes: Die Gesamtmenge der übertragenen eingehenden Daten (in Gigabyte).
- Amazon Lightsail Region-TotalDataXfer-Out-Bytes: Die Gesamtmenge der übertragenen ausgehenden Daten (in Gigabyte).
- Amazon Lightsail Region-DataXfer-Out-Overage-Bytes: Die Menge der ins Internet oder an öffentliche IP-Adressen übertragenen ausgehenden Daten, die über das Kontingent der verwendeten Instance- oder Datenbankpläne hinausgeht (in Gigabyte).

- Amazon Lightsail Region-DataXfer-Out-Free-Bytes (veraltet): Die Menge der übertragenen ausgehenden Daten, die innerhalb des Kontingents der verwendeten Instance- oder Datenbankpläne liegt (in Gigabyte).
- Amazon Lightsail Region-DataXfer-Out-Other-Bytes (veraltet): Die Menge der an private IP-Adressen übertragenen ausgehenden Daten, die über das Kontingent der verwendeten Instance- oder Datenbankpäne hinausgeht (in Gigabyte). Diese Überschreitung ist kostenlos, wenn die Übertragung an eine AWS-Ressource über eine private IP erfolgt.

Regionscodes in Ihrer Rechnung

Lightsail-Fakturierungs- und Nutzungsberichte verwenden Codes und Abkürzungen. Für den Nutzungstyp beispielsweise wird die Region durch eine der folgenden Abkürzungen ersetzt:

- Asien-Pazifik (Tokio) (ap-northeast-1)
- Asien-Pazifik (Seoul) (ap-northeast-2)
- Asien-Pazifik (Singapur) (ap-southeast-1)
- Asien-Pazifik (Sydney) (ap-southeast-2)
- Asien-Pazifik (Mumbai) (ap-south-1)
- Kanada (Zentral) (ca-central-1)
- EU (Irland) (eu-west-1)
- EU (Frankfurt) (eu-central-1)
- EU (London) (eu-west-2)
- EUW3: Paris (eu-west-3)
- EUN1 (Stockholm) eu-north-1
- USA Ost (Nord-Virginia) (us-east-1)
- USA Ost (Ohio) (us-east-2)
- USA West (Oregon) (us-west-2)

Häufig gestellte Fragen in Lightsail

Dieses Thema beantwortet häufig gestellte Fragen (FAQ). Wenn Sie eine häufig gestellte Frage haben, die hier nicht beantwortet wurde, verwenden Sie die Fragen? Kommentare? Feedback-Schaltfläche, unten auf der Seite. Sie können auch eine Frage im Lightsail-Diskussionsforum stellen.

Inhalt

Allgemeines

Was ist Amazon Lightsail?

> Amazon Lightsail ist der einfachste Einstieg AWS für Entwickler, kleine Unternehmen, Studenten und andere Benutzer, die eine Lösung benötigen, um ihre Websites und Webanwendungen in der Cloud zu erstellen und zu hosten. Lightsail bietet Entwicklern Rechen-, Speicher- und

Netzwerkkapazität. Lightsail bietet alles, was Sie benötigen, um Ihr Projekt schnell zu starten — virtuelle Maschinen, Container, Datenbanken, CDN, Load Balancer, DNS-Management usw. — zu einem niedrigen, vorhersehbaren monatlichen Preis.

Was kann ich mit Lightsail machen?

Sie können vorkonfigurierte virtuelle private Server (Instanzen) erstellen, die alles enthalten, um Ihre Anwendung einfach bereitzustellen und zu verwalten, oder Datenbanken erstellen, für die die Sicherheit und Integrität der zugrunde liegenden Infrastruktur und des Betriebssystems von Lightsail verwaltet wird. Lightsail eignet sich am besten für Projekte, die ein paar Dutzend Instanzen oder weniger benötigen, und für Entwickler, die eine einfache Verwaltungsoberfläche bevorzugen. Zu den häufigsten Anwendungsfällen für Lightsail gehören das Ausführen von Websites, Webanwendungen, Unternehmenssoftware, Blogs, E-Commerce-Websites und mehr. Wenn Ihr Projekt wächst, können Sie Load Balancer und angeschlossenen Blockspeicher zusammen mit Ihrer Instance verwenden, um die Redundanz und Verfügbarkeit zu erhöhen und auf Dutzende anderer AWS Dienste zuzugreifen, um neue Funktionen hinzuzufügen.

Bietet Lightsail eine API an?

Ja. Alles, was Sie in der Lightsail-Konsole tun, wird von einer öffentlich verfügbaren API unterstützt. Erfahren Sie, wie Sie die Lightsail-CLI und -API installieren und verwenden.

Wie melde ich mich bei Lightsail an?

Um Lightsail zu verwenden, wählen Sie Get Started und melden Sie sich an. Sie verwenden Ihr Amazon Web Services Services-Konto, um auf Lightsail zuzugreifen. Falls Sie noch keines haben, werden Sie aufgefordert, eines zu erstellen.

In welchem AWS-Region s ist Lightsail erhältlich?

Lightsail ist derzeit in allen Availability Zones in den folgenden AWS-Region s verfügbar:

- USA Ost (Ohio): (us-east-2)
- USA Ost (Nord-Virginia): (us-east-1)
- USA West (Oregon): (us-west-2)
- Asien-Pazifik (Mumbai): (ap-south-1)
- Asien-Pazifik (Seoul): (ap-northeast-2)
- Asien-Pazifik (Singapur): (ap-southeast-1)

- Asien-Pazifik (Sydney): (ap-southeast-2)
- Asien-Pazifik (Tokio): (ap-northeast-1)
- Kanada (Zentral): (ca-central-1)
- EU (Frankfurt): (eu-central-1)
- EU (Irland): (eu-west-1)
- EU (London): (eu-west-2)
- EU (Paris): (eu-west-3)
- Europa (Stockholm) (eu-north-1)

Weitere Informationen finden Sie unter AWS-Region s und Availability Zones in Lightsail.

Was sind Availability Zones?

Availability Zones sind Gruppen von Rechenzentren, die auf einer physisch separierten, unabhängigen Infrastruktur ausgeführt werden und auf höchste Zuverlässigkeit ausgelegt sind. Generatoren oder Kühlsysteme, also mögliche Fehlerquellen, versorgen stets nur eine Availability Zone. Darüber hinaus sind Availability Zones physisch separiert, sodass selbst extrem unwahrscheinliche Gefahren wie Feuer, Tornados oder Überflutungen jeweils nur eine einzelne Availability Zone betreffen können.

Was sind die Lightsail-Servicekontingente?

Die neuesten Lightsail-Dienstkontingente, einschließlich der Kontingente, die erhöht werden können, finden Sie unter Lightsail-Dienstkontingente in der. Allgemeine AWS-Referenz Wenn Sie ein Kontingent erhöhen müssen, eröffnen Sie bitte einen Fall beim AWS Support.

Wie erhalte ich weitere Hilfe?

Wir sind für Sie da. Unser kontextsensitives Hilfefenster in Lightsail bietet sofort hilfreiche Tipps zu Ihren Aktionen in der Konsole. Von der Lightsail-Konsole aus können Sie auch auf eine Bibliothek mit Anleitungen, Übersichten und Anleitungen für die ersten Schritte zugreifen. Und wenn Sie die Lightsail-API oder AWS CLI verwenden möchten, bietet Lightsail eine vollständige API-Referenz für alle unterstützten Programmiersprachen. Sie können auch die Lightsail-Supportressourcen nutzen.

Wenn Sie ein Problem mit Ihrem Konto oder zur Abrechnung haben, wenden Sie sich online an den AWS Support. Mit Ihrem Lightsail-Konto erhalten Sie rund um die Uhr kostenlosen Zugriff.

Wenn Sie eine allgemeine Frage zur Verwendung von Lightsail haben, suchen Sie in der Lightsail-Dokumentation und in den Support-Foren.

Darüber hinaus bietet AWS Support eine Reihe von kostenpflichtigen Tarifen, um Ihre individuellen Bedürfnisse abzudecken.

Instances

Was ist eine Lightsail-Instanz?

Eine Lightsail-Instanz ist ein virtueller privater Server (VPS), der sich in der Cloud befindet. AWS Verwenden Sie Ihre Lightsail-Instanzen, um Ihre Daten zu speichern, Ihren Code auszuführen und webbasierte Anwendungen oder Websites zu erstellen. Ihre Instances können sowohl über öffentliche (Internet) als auch über private (VPC) Netzwerke miteinander und mit anderen AWS Ressourcen verbunden werden. Sie können Instances einfach direkt von der Lightsail-Konsole aus erstellen, verwalten und eine Verbindung zu ihnen herstellen.

Was ist ein Lightsail-Tarif?

Ein Lightsail-Plan, der auch als Paket bezeichnet wird, umfasst einen virtuellen Server mit einer festen Menge an Arbeitsspeicher (RAM) und Rechenleistung (vCPUs), SSD-basiertem Speicher (Festplatten) und einer kostenlosen Datenübertragungslizenz. Lightsail-Pläne bieten auch statische IPv4-Adressen und DNS-Management. Lightsail-Tarife werden stündlich und auf Abruf abgerechnet, sodass Sie nur für einen Tarif zahlen, wenn Sie ihn nutzen.

Welche Software kann ich auf meinen Instances ausführen?

Lightsail bietet eine Reihe von Betriebssystem- und Anwendungsvorlagen, die automatisch installiert werden, wenn Sie eine neue Lightsail-Instanz erstellen. Zu den Anwendungsvorlagen gehören WordPress Multisite WordPress, cPanel & WHM, Django, Drupal, Ghost PrestaShop, Joomla! , Magento, Redmine, LAMP, Nginx (LEMP), MEAN und Node.js.

Unter Verwendung des SSH-Clients in Ihrem Browser oder Ihres eigenen SSH-Clients können Sie auf Ihren Instances zusätzliche Software installieren.

Welche Betriebssysteme kann ich mit Amazon Lightsail verwenden?

Lightsail unterstützt derzeit 7 Linux- oder UNIX-ähnliche Distributionen: AlmaLinux OS 9, Amazon Linux 2, Amazon Linux 2023, CentOS, Debian, FreeBSD, openSUSE und Ubuntu sowie drei Windows Server-Versionen: 2016, 2019 und 2022.

Muss ich meine eigene Lizenz mitbringen, um Lightsail-Instanzen nutzen zu können?

Alle auf Lightsail verfügbaren Instanz-Blueprints enthalten eine Lizenz, mit Ausnahme des cPanel- und WHM-Blueprints. Diese Vorlage beinhaltet eine 15-tägige Testlizenz. Weitere Informationen finden Sie in der Schnellstartanleitung: cPanel & WHM auf Amazon Lightsail. Für alle anderen Instance-Vorlagen müssen Sie keine eigene Lizenz (BYOL, Bring-Your-Own-License) mitbringen.

Wie erstelle ich eine Lightsail-Instanz?

Nachdem Sie sich bei Lightsail angemeldet haben, können Sie die Lightsail-Konsole, die Befehlszeilenschnittstelle (CLI) oder die API verwenden, um Instanzen zu erstellen und zu verwalten.

Wenn Sie sich zum ersten Mal bei der Konsole anmelden, wählen Sie „Instance erstellen“. Auf der Seite „Instance erstellen“ können Sie die Software, den Speicherort und den Namen für Ihre Instance wählen. Sobald Sie Ihre „Erstellen“ gewählt haben, wird Ihre neue Instance automatisch innerhalb weniger Minuten angelegt.

Wie funktionieren Lightsail-Instances?

Lightsail-Instances wurden speziell AWS für Webserver, Entwicklerumgebungen und kleine Datenbankanwendungsfälle entwickelt. Solche Workloads verwenden häufig nicht oder nicht durchgängig die volle CPU-Leistung, verursachen jedoch gelegentlich Spitzenlasten. Lightsail verwendet Burstable-Performance-Instances, die ein Basisniveau an CPU-Leistung bieten und zusätzlich die Möglichkeit bieten, über dem Basiswert zu liegen. Dadurch erhalten Sie die Leistung, die Sie benötigen, wenn Sie sie benötigen, schützen sich aber zugleich vor der schwankenden Leistung und anderen häufigen Nebenwirkungen, die in anderen Umgebungen bei überdimensionierten Abonnements typischerweise auftreten.

Wenn Sie hochkonfigurierbare Umgebungen und Instances mit gleichbleibend hoher CPU-Leistung für Anwendungen wie Videokodierung oder HPC-Anwendungen benötigen, empfehlen wir die Nutzung von Amazon EC2.

Woher weiß ich, wann meine Instances überlastet werden?

Das Diagramm der CPU-Auslastungsmetrik für Ihre Instance enthält eine nachhaltige Zone und eine burstfähige Zone. Ihre Lightsail-Instance kann unbegrenzt in der nachhaltigen Zone arbeiten, ohne dass dies Auswirkungen auf den Betrieb Ihres Systems hat. Ihre Instance kann bei starker Belastung in der burstfähigen Zone arbeiten. Bei Betrieb in der burstfähigen Zone ruft Ihre Instance eine höhere Anzahl von CPU-Zyklen ab. Daher kann sie nur begrenzte Zeit in dieser Zone betrieben werden. Weitere Informationen finden Sie unter Instance-Metriken in Amazon Lightsail anzeigen.

Fügen Sie einen Metrik-Alarm hinzu, damit Sie benachrichtigt werden, wenn die CPU-Auslastung Ihrer Instance die Grenze zwischen der nachhaltigen Zone und der burstfähigen Zone überschreitet. Weitere Informationen finden Sie unter Alarme für Instance-Metriken in Amazon Lightsail erstellen.

Wie stelle ich eine Verbindung zu einer Lightsail-Instance her?

Lightsail bietet direkt von Ihrem Browser aus eine sichere 1-Klick-Verbindung zum Terminal Ihrer Instanz und unterstützt SSH-Zugriff für Linux/UNIX-basierte Instances und RDP-Zugriff für Windows-basierte Instances. Wenn Sie 1-Klick-Verbindungen verwenden möchten, starten Sie Ihre Instance-Verwaltungsbildschirme und wählen Sie Connect using SSH (Mit SSH verbinden) oder Connect using RDP (Mit RDP verbinden). Ein neues Browser-Fenster wird geöffnet und es wird automatisch eine Verbindung mit Ihrer Instance eingerichtet.

Wenn Sie es vorziehen, über Ihren eigenen Client eine Verbindung zu Ihrer Linux/UNIX-basierten Instance herzustellen, erledigt Lightsail die Speicherung und Verwaltung der SSH-Schlüssel für Sie und stellt Ihnen einen sicheren Schlüssel zur Verfügung, den Sie in Ihrem SSH-Client verwenden können.

Wie kann ich meine Instances sichern?

Wenn Sie Ihre Daten sichern möchten, können Sie die Lightsail-Konsole oder API verwenden, um einen manuellen Snapshot Ihrer Instanz zu erstellen, oder automatische Snapshots aktivieren, damit Lightsail täglich Snapshots für Sie erstellt. Wenn es zu einem Ausfall kommt oder fehlerhafter Code bereitgestellt wird, können Sie später Ihren Instance-Snapshot verwenden, um eine völlig neue Instance zu erstellen. Weitere Informationen finden Sie unter Snapshots.

Kann ich meinen Plan erweitern?

Ja. Sie können einen Snapshot Ihrer Instance verwenden, um eine neue, größere Instance zu erstellen. Weitere Informationen finden Sie unter Snapshots.

Wie kann ich Lightsail-Instanzen mit anderen Ressourcen in meinem AWS Konto verbinden?

Sie können Ihre Lightsail-Instances mithilfe von VPC-Peering privat mit Amazon VPC-Ressourcen in Ihrem AWS Konto verbinden. Wählen Sie einfach auf Ihrer Lightsail-Kontoseite die Option VPC-Peering aktivieren aus, und Lightsail erledigt die Arbeit für Sie. Sobald VPC-Peering aktiviert ist, können Sie andere AWS Ressourcen in Ihrer standardmäßigen Amazon-VPC mithilfe ihrer privaten IPs adressieren. Anweisungen finden Sie hier.

> **Note**
>
> Beachten Sie, dass Sie in Ihrem AWS Konto eine Standard-Amazon-VPC eingerichtet haben müssen, damit VPC-Peering mit Lightsail funktioniert. AWS Konten, die vor Dezember 2013 erstellt wurden, haben keine Standard-VPC, und Sie müssen eine einrichten. Weitere Informationen zu der Einrichtung Ihrer Standard-VPC finden Sie hier.

Was ist der Unterschied zwischen dem Anhalten und dem Löschen meiner Instance?

Wenn Sie Ihre Instance anhalten, wird sie in ihrem aktuellen Status heruntergefahren und Sie können sie jederzeit neu starten. Durch das Anhalten Ihrer Instance wird ihre öffentliche IPv4-Adresse freigegeben. Daher wird empfohlen, dass Sie die statische IPv4-Adressen für Instances verwenden, die nach dem anhalten und starten wieder dieselbe IP erhalten müssen. Beachten Sie, dass sich die öffentlichen IPv6-Adressen, die an Instances angefügt sind, nicht ändern, selbst wenn Instances angehalten und gestartet werden.

Wenn Sie Ihre Instance löschen, ist dies eine endgültige Aktivität. Wenn Sie keinen Instance-Snapshot erstellt haben, gehen alle Ihre Instance-Daten verloren und können nicht wiederhergestellt werden. Automatische Snapshots werden auch mit der Instance gelöscht, es sei denn, Sie behalten sie, indem Sie sie als manuelle Snapshots kopieren. Die öffentlichen und privaten IP-Adressen der Instance werden ebenfalls freigegeben. Wenn Sie eine statische IPv4-Adresse für diese Instance verwendet haben, wird die statische IPv4-Adresse davon getrennt, verbleibt aber in Ihrem Konto.

Objektspeicher und Buckets

Was kann ich mit der Lightsail-Objektspeicherung machen?

Sie können Ihre statischen Inhalte wie Images, Videos und HTML-Dateien in einem Bucket im Lightsail-Objektspeicherdienst speichern. Sie können die in Ihrem Bucket gespeicherten Objekte mit Ihren Websites und Anwendungen verwenden. Lightsail-Objektspeicher kann mit wenigen einfachen Klicks Ihrer Lightsail-CDN-Verteilung zugeordnet werden, wodurch die Bereitstellung Ihrer Inhalte für ein globales Publikum schnell und einfach beschleunigt werden kann. Es kann auch als kostengünstige, sichere Backup-Lösung verwendet werden. Weitere Informationen finden Sie unter Objektspeicher.

Wie viel kostet der Lightsail-Objektspeicher?

Lightsail Object Storage bietet in allen Ländern, in denen Lightsail erhältlich ist, drei verschiedene Pakete zum Festpreis AWS-Region. Das erste Bündel ist 1 USD/Monat und ist für die ersten 12 Monate kostenlos. Dieses Bündel enthält 5 GB Speicherkapazität und 25 GB Datenübertragung. Das zweite Bündel kostet 3 USD pro Monat und umfasst 100 GB Speicherkapazität und 250 GB Datenübertragung. Das dritte Bündel kostet 5 USD pro Monat und umfasst 250 GB Speicherkapazität und 500 GB Datenübertragung. Lightsail-Objektspeicher beinhaltet unbegrenzte Datenübertragung in Ihren Bucket, da die gebündelte Datenübertragungszulage nur für die Datenübertragung aus Ihrem Bucket verwendet wird.

Hat der Lightsail-Objektspeicher Überschreitungsgebühren?

Wenn Sie die monatliche Speicherkapazität oder Datenübertragungszulage Ihres Objektspeicherplans für einen einzelnen Bucket überschreiten, wird Ihnen der zusätzliche Betrag in Rechnung gestellt. Weitere Informationen finden Sie in der Lightsail-Preisliste.

Wie funktioniert meine Datenübertragungszulage mit dem Objektspeicher?

Sie können Ihre Datenübertragungszulage nutzen, indem Sie Daten in und aus dem Lightsail-Objektspeicher übertragen, mit folgenden Ausnahmen:

- Daten, die aus dem Internet in den Lightsail-Objektspeicher übertragen werden
- Datenübertragung zwischen Lightsail-Objektspeicherressourcen
- Daten, die aus dem Lightsail-Objektspeicher an eine andere Lightsail-Ressource in demselben übertragen wurden AWS-Region (einschließlich an eine Ressource in einem anderen AWS Konto, aber in demselben) AWS-Region
- Daten, die aus dem Lightsail-Objektspeicher in eine Lightsail-CDN-Verteilung übertragen werden

Kann ich den Plan ändern, der mit meinem Lightsail-Bucket verknüpft ist?

Ja, Sie können den Speicherplan eines einzelnen Lightsail-Buckets einmal innerhalb Ihres monatlichen AWS Abrechnungszeitraums ändern.

Kann ich Objekte aus dem Lightsail -Objektspeicher in Amazon S3 kopieren?

Ja, das Kopieren vom Lightsail-Objektspeicher in Amazon S3 wird unterstützt. Weitere Informationen finden Sie unter Wie kann ich alle Objekte von einem Amazon-S3-Bucket in einen anderen Bucket kopieren? im AWS Premium Support Knowledge Center.

Was sind die ersten Schritte mit dem Lightsail-Objektspeicher?

Um den Lightsail-Objektspeicher zu verwenden, müssen Sie zunächst einen Bucket erstellen, der zum Speichern der Daten verwendet wird. Weitere Informationen finden Sie unter Einen Bucket erstellen. Nachdem Ihr Bucket betriebsbereit ist, können Sie mit dem Hinzufügen von Objekten zu Ihrem Bucket beginnen, indem Sie Dateien über die Lightsail-Konsole hochladen oder Ihre Anwendung so konfigurieren, dass Inhalte wie Protokolle oder andere Anwendungsdaten in den Bucket eingefügt werden. Alternativ können Sie auch mithilfe von AWS Command Line Interface ()AWS CLI mit Lightsail-Objektspeicher beginnen.

Wie lade ich Objekte in meinen Bucket hoch?

Um Objekte wie Images oder andere statische Dateien in Ihren Bucket hochzuladen, wählen Sie „Hochladen“ aus der oberen Navigationsleiste „Objekte“ und wählen Sie die richtige Datei oder das richtige Verzeichnis von Ihrem Computer aus. Alternativ können Sie Dateien und Verzeichnisse von Ihrem Desktop in den markierten Bereich in der Lightsail-Objektspeicher-Konsole ziehen und ablegen.

Kann ich den öffentlichen Zugriff auf meinen Bucket blockieren?

Lightsail-Buckets und -Objekte sind standardmäßig auf „privat“ festgelegt, was bedeutet, dass nur Benutzer mit entsprechenden Berechtigungen Zugriff auf den Bucket und die Objekte haben. Ein Benutzer kann diese Standardeinstellung ändern und einzelne Objekte in einem privaten Bucket öffentlich und schreibgeschützt machen oder den gesamten Bucket öffentlich und schreibgeschützt machen. Wenn ein Benutzer einen Bucket oder ein Objekt öffentlich macht, kann jeder auf der Welt seinen Inhalt lesen. Weitere Informationen finden Sie unter Bucketberechtigungen.

Wie gewähre ich programmatischen Zugriff auf meinen Bucket?

Sie können entweder Zugriffsschlüssel oder Rollen für den programmatischen Zugriff auf Ihren Bucket verwenden. Wählen Sie zunächst den Bucket aus, mit dem Sie programmatisch eine Verbindung zur Lightsail-Konsole herstellen möchten. Erstellen Sie anschließend auf der Registerkarte Berechtigungen einen Zugriffsschlüssel oder weisen Sie Ihrer Lightsail-Instanz eine Rolle zu und konfigurieren Sie dann Ihre Website oder Ihren Anwendungscode für die Verwendung Ihres Buckets. Dieses Verhalten kann je nachdem, wie Sie den Objektspeicher mit Ihrer Website oder Anwendung verwenden möchten, variieren. Weitere Informationen finden Sie unter Bucketberechtigungen.

Wie teile ich einen Bucket mit anderen AWS Konten?

Lightsail erleichtert die kontoübergreifende gemeinsame Nutzung, indem Sie den Zugriff auf Ihren Bucket mit der AWS Konto-ID teilen können, die Sie im Abschnitt Kontoübergreifender Zugriff der Bucket-Verwaltungsseite angeben. Nachdem Sie eine AWS Konto-ID angegeben haben, hat dieses Konto nur Lesezugriff auf den Bucket. Weitere Informationen finden Sie unter Bucketberechtigungen.

Was ist Versioning?

Mit Versioning können Sie alle Versionen aller Objektspeicher in Ihrem Bucket beibehalten, abrufen und wiederherstellen. Dies bietet einen zusätzlichen Schutz vor versehentlichen Überschreibungen und Löschungen. Weitere Informationen finden Sie unter Aktivieren und Aussetzen der Bucket-Objekt-Versionsverwaltung.

Wie verbinde ich meinen Lightsail-Bucket mit meiner Lightsail-CDN-Verteilung?

Lightsail-Objektspeicher kann mit wenigen einfachen Klicks Ihrer Lightsail-CDN-Verteilung zugeordnet werden, wodurch die Bereitstellung Ihrer Inhalte für ein globales Publikum schnell und einfach beschleunigt werden kann. Erstellen Sie dazu eine Lightsail-CDN-Verteilung und wählen Sie einfach den Lightsail-Bucket als Ursprung Ihrer Lightsail-CDN-Verteilung aus. Weitere Informationen finden Sie unter Verwenden eines Amazon-Lightsail-Buckets mit einer Netzwerkverteilungen für die Bereitstellung von Inhalten.

Welche Grenzwerte gibt es für den Lightsail-Objektspeicherdienst?

Sie können bis zu 20 Buckets im Lightsail-Objektspeicherdienst pro Konto erstellen. Die Anzahl der Objekte, die Sie in einem Bucket speichern können, ist nicht begrenzt. Sie können alle Ihre Objekte in einem einzigen Bucket speichern, oder sie über mehrere Buckets verteilen.

Unterstützt Lightsail-Objektspeicher Überwachung und Warnungen?

Mit dem Lightsail-Objektspeicher können Kunden ganz einfach Metriken zum gesamten belegten Speicherplatz innerhalb eines Buckets und die Anzahl der Objekte innerhalb des Buckets anzeigen. Warnungen basierend auf diesen Metriken werden ebenfalls unterstützt. Weitere Informationen finden Sie unter Metriken für Ihren Bucket in Amazon Lightsail anzeigen und Bucket-Metrik-Alarme erstellen.

Container-Services

Was kann ich mit Lightsail-Containerdiensten machen?

Lightsail-Container-Services bieten eine einfache Möglichkeit, containerisierte Anwendungen in der Cloud auszuführen. Sie können eine Vielzahl von Anwendungen auf einem Container-Service ausführen, von einfachen Web-Apps bis hin zu mehrstufigen Mikrodiensten. Sie geben lediglich das Container-Image, die Leistung (CPU, RAM) und den Umfang (Anzahl der Knoten) an, die für Ihren Container-Service erforderlich sind. Lightsail kümmert sich um den Betrieb des Containerdienstes, ohne dass Sie die zugrunde liegende Infrastruktur verwalten müssen. Lightsail stellt Ihnen einen TLS-Endpunkt mit Lastenausgleich für den Zugriff auf die Anwendung zur Verfügung, die auf dem Container-Service ausgeführt wird.

Kann der Lightsail-Containerdienst Docker-Container ausführen?

Ja. Lightsail unterstützt Linux-basierte Docker-Container. Windows-Container werden derzeit nicht unterstützt.

Wie verwende ich meine öffentlichen Container-Images mit dem Lightsail-Container-Service?

Sie können Container-Images aus einer öffentlichen Online-Registry wie Amazon ECR Public Registry verwenden oder Ihr eigenes benutzerdefiniertes Image erstellen und es mit dem in wenigen einfachen Schritten an Lightsail übertragen. AWS CLI Weitere Informationen finden Sie unter Übertragen und Verwalten von Container-Images.

Kann ich meine Container-Images aus einer privaten Container-Registry ziehen?

Derzeit werden nur öffentliche Container-Registries von Lightsail-Containerdiensten unterstützt. Alternativ können Sie Ihre benutzerdefinierten Container-Images von Ihrem lokalen Computer zu Lightsail übertragen, um sie privat zu halten.

Kann ich die Leistung und die Skalierung meines Dienstes je nach Bedarf ändern?

Ja, die Leistung und Skalierung von Containern können jederzeit geändert werden, auch nachdem der Dienst erstellt wurde.

Kann ich den Namen des vom Lightsail-Container-Service erstellten HTTPS-Endpunkts anpassen?

Lightsail bietet einen HTTPS-Endpunkt für jeden Container-Service im Format. `<service-name>.<random-guid>.<aws-region-name>.cs.amazonlightsail.com` Es kann nur der Dienstname angepasst werden. Alternativ können Sie einen benutzerdefinierten Domänennamen verwenden. Weitere Informationen finden Sie unter Aktivieren und verwalten benutzerdefinierter Domains.

Kann ich benutzerdefinierte Domains für den HTTPS-Endpunkt eines Lightsail-Containerdienstes verwenden?

Ja. Sie können ein SSL/TLS-Zertifikat mit benutzerdefinierten Domainnamen erstellen und an Ihren Container-Service in Lightsail anhängen. Die Zertifikate müssen domänenvalidiert sein. Wenn das DNS Ihrer Domain eine Lightsail-DNS-Zone verwendet, können Sie den Traffic für den Apex Ihrer Domain (`example.com`) oder einer Subdomain (`www.example.com`) an Ihre Container-Services weiterleiten. Alternativ können Sie einen DNS-Hosting-Anbieter verwenden, der das Hinzufügen von ALIAS-Einträgen unterstützt, um den Apex Ihrer Domain (`example.com`) der Standarddomain (Public DNS) Ihres Lightsail-Containerdienstes zuzuordnen. Weitere Informationen finden Sie unter Aktivieren und verwalten benutzerdefinierter Domains.

Was kosten Lightsail-Containerdienste?

Lightsail-Containerdienste werden nach einem On-Demand-Stundensatz abgerechnet, sodass Sie nur für das bezahlen, was Sie tatsächlich nutzen. Für jeden Lightsail-Containerdienst, den Sie nutzen, berechnen wir Ihnen den festen Stundenpreis bis zum monatlichen Höchstpreis. Der maximale monatliche Dienstpreis kann berechnet werden, indem der Basispreis der Leistung Ihres Dienstes mit der Skala Ihres Dienstes multipliziert wird. Beispielsweise kostet ein Dienst mit Micro-Leistung und Skalierung von 2 maximal $10*2=$20/Monat. Der günstigste Lightsail-Containerdienst beginnt bei 0,0094 USD/Stunde (7 USD/Monat). Für die Nutzung über dem freien Kontingent von 500 GB pro Monat für jeden Dienst können zusätzliche Datenübertragungskosten anfallen.

Wird mir der ganze Monat in Rechnung gestellt, auch wenn ich meinen Container-Service nur für einige Tage betreibe?

Ihre Lightsail-Containerdienste werden nur dann in Rechnung gestellt, wenn sie aktiv oder deaktiviert sind. Wenn Sie Ihren Lightsail-Containerdienst vor Ende des Monats löschen, berechnen wir Ihnen anteilige Kosten, die auf der Gesamtzahl der Stunden basieren, die Sie Ihren Lightsail-Containerdienst genutzt haben. Wenn Sie beispielsweise Ihren Lightsail-Containerdienst mit einer Leistung von Micro und einer Skala von 1 für 100 Stunden pro Monat nutzen, werden Ihnen 1,34 USD (0,0134 USD*100) berechnet.

Wird mir die Datenübertragung in und aus dem Container-Service in Rechnung gestellt?

Jeder Container-Service verfügt über ein Datenübertragungskontingent (500 GB pro Monat). Dies gilt sowohl für die Datenübertragung IN als auch AUS Ihrem Dienst. Wenn Sie das Kontingent überschreiten, wird Ihnen die ausgehende Datenübertragung von einem Lightsail-Containerdienst ins Internet oder zu einem anderen AWS-Region oder zu AWS Ressourcen in derselben Region

in Rechnung gestellt, wenn Sie öffentliche IP-Adressen verwenden. Die Gebühr für diese Art von Datenübertragung über das kostenlose Kontingent hinaus beträgt:

- USA Ost (Ohio) (us-east-2): 0,09 USD/GB
- USA Ost (Nord-Virginia): (us-east-1): 0,09 USD/GB
- USA West (Oregon): (us-west-2): 0,09 USD/GB
- Asien-Pazifik (Mumbai): (ap-south-1): 0,13 USD/GB
- Asien-Pazifik (Seoul): (ap-northeast-2): 0,13 USD/GB
- Asien-Pazifik (Singapur): (ap-southeast-1): 0,12 USD/GB
- Asien-Pazifik (Sydney): (ap-southeast-2): 0,17 USD/GB
- Asien-Pazifik (Tokio): (ap-northeast-1): 0,14 USD/GB
- Kanada (Zentral): (ca-central-1): 0,09 USD/GB
- EU (Frankfurt): (eu-central-1): 0,09 USD/GB
- EU (Irland): (eu-west-1): 0,09 USD/GB
- EU (London): (eu-west-2): 0,09 USD/GB
- EU (Paris): (eu-west-3): 0,09 USD/GB
- Europa (Stockholm) (eu-north-1): 0,09 USD/GB

Was ist der Unterschied zwischen dem Anhalten und dem Löschen meines Container-Servicess?

Wenn Sie Ihren Container-Service deaktivieren, befinden sich die Containerknoten in einem deaktivierten Zustand, und der öffentliche Endpunkt des Dienstes gibt einen HTTP-Statuscode '503' zurück. Durch Aktivieren des Dienstes wird der Dienst in der letzten aktiven Bereitstellung wiederhergestellt. Leistungs- und Skalierungskonfigurationen bleiben ebenfalls erhalten. Der Name des öffentlichen Endpunkts ändert sich nach der erneuten Aktivierung nicht. Bereitstellungsverlauf und Container-Images bleiben erhalten.

Wenn Sie Ihren Container-Service löschen, führen Sie eine zerstörerische Handlung aus. Alle Container-Knoten des Dienstes werden dauerhaft gelöscht. Die öffentliche HTTPS-Endpunktadresse, Container-Images, Bereitstellungsverlauf und Protokolle, die mit Ihrem Dienst

verknüpft sind, werden ebenfalls endgültig gelöscht. Sie können die Endpunktadresse nicht wiederherstellen.

Wird mir mein Container-Service in einem deaktivierten Zustand berechnet?

Ja, Ihnen wird entsprechend der Konfiguration des Container-Servicess und der Skalierung eine Rechnung gestellt, selbst wenn dieser sich in einem deaktivierten Zustand befindet.

Kann ich Containerdienste als Ausgangspunkt für meine Lightsail Content Delivery Network (CDN) - Distributionen verwenden?

Containerdienste werden derzeit nicht als Ursprung für Lightsail-CDN-Distributionen unterstützt.

Kann ich Containerdienste als Ziele für meinen Lightsail Load Balancer verwenden?

Nein. Containerdienste sind derzeit nicht als Ziele für Lightsail-Loadbalancer verfügbar. Die öffentlichen Endpunkte von Container-Services verfügen jedoch über eine integrierte Load Balancer.

Kann ich den öffentlichen Endpunkt meines Container-Servicess so konfigurieren, dass HTTP-Anfragen an HTTPS umgeleitet werden?

Öffentliche Endpunkte des Lightsail-Containerdienstes leiten automatisch alle HTTP-Anfragen an HTTPS weiter, um sicherzustellen, dass Ihre Inhalte sicher bereitgestellt werden.

Unterstützen Container-Services Überwachung und Warnungen?

Container-Services bieten Metriken für die CPU-Auslastung und die Speicherauslastung über die Knoten Ihres Dienstes hinweg. Warnungen basierend auf diesen Metriken werden derzeit nicht unterstützt.

Unterstützen Lightsail-Containerdienste IPv6?

Die HTTPS-Endpunkte des Lightsail-Containerdienstes unterstützen sowohl IPv4 als auch IPv6. Pv6 kann auf Container-Servicesn nicht deaktiviert werden.

Datenbanken

Was sind von Lightsail verwaltete Datenbanken?

Von Lightsail verwaltete Datenbanken sind Instanzen, die ausschließlich für den Betrieb von Datenbanken und nicht für andere Workloads wie Webserver, Mailserver usw. vorgesehen sind. Eine verwaltete Datenbank kann mehrere benutzerseitig erstellte Datenbanken enthalten, auf die

Sie zugreifen können, indem Sie dieselben Tools und Anwendungen wie bei einer eigenständigen Datenbank verwenden. Lightsail gewährleistet die Sicherheit und Integrität der Ihrer Datenbank zugrunde liegenden Infrastruktur und des Betriebssystems, sodass Sie eine Datenbank auch ohne umfassende Kenntnisse im Infrastrukturmanagement betreiben können.

Wie normale Lightsail-Instanzen enthalten auch die von Lightsail verwalteten Datenbanken eine feste Menge an Arbeitsspeicher, Rechenleistung und SSD-basiertem Speicher in ihren Plänen, die Sie im Laufe der Zeit skalieren können. Lightsail installiert und konfiguriert die von Ihnen gewählte Datenbank bei der Erstellung automatisch für Sie.

Was kann ich mit verwalteten Lightsail-Datenbanken machen?

Mit Lightsail verwaltete Datenbanken bieten eine einfache und wartungsarme Möglichkeit, Ihre Daten in der Cloud zu speichern. Sie können verwaltete Datenbanken entweder als neue Datenbank ausführen oder indem Sie von einer vorhandenen lokalen oder gehosteten Datenbank zu Lightsail migrieren.

Sie können auch die Skalierung Ihrer Anwendung für größere Datenverkehrsvolumina und intensivere Lasten zulassen, indem Sie Ihre Datenbank auf eine Dedicated Instance auslagern. Von Lightsail verwaltete Datenbanken sind besonders nützlich für statusbehaftete Anwendungen — wie WordPress die gängigsten CMS —, bei denen Daten synchron gehalten werden müssen, wenn Sie über eine einzelne Instanz hinaus skalieren. Verwaltete Datenbanken können mit einem Lightsail-Load Balancer und zwei oder mehr Lightsail-Instanzen kombiniert werden, um eine leistungsstarke, skalierte Anwendung zu erstellen. Durch die Verwendung verwalteter Lightsail-Datenbankpläne mit hoher Verfügbarkeit können Sie Ihrer Datenbank auch Redundanz hinzufügen und so eine hohe Verfügbarkeit Ihrer Anwendung sicherstellen.

Was verwaltet Lightsail für mich?

Lightsail verwaltet eine Reihe von Wartungsaktivitäten und Sicherheitsvorkehrungen für Ihre verwaltete Datenbank und die zugrunde liegende Infrastruktur. Lightsail sichert Ihre Datenbank automatisch und ermöglicht mithilfe des Datenbankwiederherstellungstools eine Point-in-Time-Wiederherstellung der letzten 7 Tage, um vor Datenverlust oder Komponentenausfällen zu schützen. Lightsail verschlüsselt außerdem automatisch Ihre Daten im Ruhezustand und bei der Übertragung, um die Sicherheit zu erhöhen, und speichert Ihr Datenbankkennwort für einfache und sichere Verbindungen zu Ihrer Datenbank. Auf der Wartungsseite führt Lightsail die Wartung Ihrer Datenbank während des festgelegten Wartungsfensters durch. Diese Wartung umfasst automatische Upgrades auf die neueste Minor-Datenbankversion und die gesamte Verwaltung der zugrundeliegenden Infrastruktur und des Betriebssystems.

Welche Arten von Datenbanken und welche Versionen dieser Datenbanken unterstützt Lightsail?

Von Lightsail verwaltete Datenbanken unterstützen die neuesten Hauptversionen von MySQL und PostgreSQL. Derzeit sind dies die Versionen MySQL 5.7, MySQL 8.0, PostgreSQL 9, PostgreSQL 10, PostgreSQL 11 und PostgreSQL 12. Lightsail bietet nur die neueste Nebenversion für jede Hauptversionsoption.

Welche verwalteten Datenbankpläne bietet Lightsail an?

Lightsail bietet verwaltete Datenbanken in 4 Größen in Standard- und Hochverfügbarkeitsplänen. Jeder Plan beinhaltet eine fest Menge Speicherplatz und ein monatliches Datentransferkontingent. Sie können außerdem bei Bedarf auf größere Pläne skalieren und zwischen Standard- und Hochverfügbarkeitsplänen wechseln. Hochverfügbarkeitspläne bieten die gleichen Ressourcen wie Standardpläne und beinhalten zusätzlich eine Standby-Datenbank, die in einer von Ihrer primären Datenbank getrennten Availability Zone ausgeführt wird, um Redundanz zu gewährleisten.

Was ist ein Hochverfügbarkeitsplan?

Von Lightsail verwaltete Datenbanken sind in Standard- und Hochverfügbarkeitsplänen erhältlich. Standard- und Hochverfügbarkeitspläne bieten identische Ressourcen, einschließlich Arbeitsspeicher, Speicherplatz und Datenübertragung. Hochverfügbarkeitspläne verleihen Ihrer Datenbank Redundanz und Beständigkeit, indem sie automatisch eine Standby-Datenbank in einer von Ihrer Primärdatenbank getrennten Availability Zone erstellen, Daten synchron in die Standby-Datenbank replizieren und bei Infrastrukturausfällen und während der Wartung einen Failover auf die Standby-Datenbank bereitstellen, sodass Sie die Verfügbarkeit auch dann sicherstellen, wenn Datenbanken automatisch von Lightsail aktualisiert/gewartet werden. Verwenden Sie Hochverfügbarkeitspläne für den Betrieb von Produktionsanwendungen oder Software, bei denen eine hohe Betriebszeit erforderlich ist.

Wie kann ich meine von Lightsail verwaltete Datenbank nach oben oder unten skalieren?

Sie können Ihre von Lightsail verwaltete Datenbank skalieren, indem Sie einen Snapshot davon erstellen und anhand des Snapshots einen neuen, größeren Datenbankplan erstellen oder indem Sie mithilfe der Notfallwiederherstellungsfunktion eine neue, größere Datenbank erstellen. Sie können außerdem von Standard- zu Hochverfügbarkeitsplänen wechseln und umgekehrt. Sie können Ihre Datenbank nicht verkleinern. Weitere Informationen finden Sie unter Erstellen einer Datenbank aus einem Snapshot in Amazon Lightsail.

Wie kann ich meine von Lightsail verwaltete Datenbank sichern?

Lightsail sichert Ihre Daten automatisch und ermöglicht die Wiederherstellung dieser Daten ab einem bestimmten Zeitpunkt in einer neuen Datenbank. Die automatische Sicherung ist ein kostenloser Service für Ihre Datenbank. Sie speichert aber nur die letzten 7 Tage der Daten. Wenn Sie Ihre Datenbank löschen, werden alle automatischen Backup-Datensätze gelöscht und eine point-in-time Wiederherstellung ist nicht mehr möglich. Um Datensicherungen nach dem Löschen Ihrer Datenbank oder ein Sicherung für mehr als 7 Tage aufzubewahren, verwenden Sie manuelle Snapshots.

Sie können auf den Datenbankverwaltungsseiten manuelle Schnappschüsse Ihrer von Lightsail verwalteten Datenbanken erstellen. Manuelle Snapshots enthalten alle Daten aus Ihrer Datenbank und können als Sicherung für Daten verwendet werden, die Sie dauerhaft speichern möchten. Sie können manuelle Snapshots außerdem verwenden, um eine neue, größere Datenbank zu erstellen oder zwischen Standard- und Hochverfügbarkeitsplänen zu wechseln. Manuelle Schnappschüsse werden gespeichert, bis Sie sie löschen. Sie werden mit 0,05 USD/GB-Monat berechnet.

Was passiert mit meinen Daten, wenn ich meine von Lightsail verwaltete Datenbank lösche?

Wenn Sie Ihre von Lightsail verwaltete Datenbank löschen, werden sowohl Ihre Datenbank selbst als auch alle automatischen Backups gelöscht. Es gibt keine Möglichkeit, diese Daten wiederherzustellen, es sei denn, Sie erstellen einen manuellen Snapshot, bevor Sie Ihre Datenbank löschen. Beim Löschen Ihrer Datenbank bietet Lightsail die Möglichkeit, mit einem Klick einen manuellen Snapshot zu erstellen, falls gewünscht, um vor versehentlichem Datenverlust zu schützen. Die Erstellung eines manuellen Snapshots vor dem Löschen ist optional, wird aber dringend empfohlen. Sie können Ihren manuellen Snapshot später löschen, wenn Sie die gespeicherten Daten nicht mehr benötigen.

Kann ich meine Instance (s) mit einer von Lightsail verwalteten Datenbank verbinden, die in verschiedenen AWS-Region s oder verschiedenen Availability Zones läuft?

Sie können von Lightsail verwaltete Datenbanken nicht mit Instanzen verwenden, die in verschiedenen AWS-Region s ausgeführt werden. Sie können in Ihrer Instance jedoch Datenbanken aus verschiedenen Availability Zones verwenden.

Wie lade ich Daten in meine von Lightsail verwaltete Datenbank?

Um Daten in Ihre von Lightsail verwaltete Datenbank zu laden, sollten Sie zunächst den Datenimportmodus aktivieren. Nachdem Sie den Datenimportmodus aktiviert haben, können Sie die Daten weiterhin manuell mit Ihrem bevorzugten Datenbank-Client hochladen. Nachdem Sie

mit dem Laden der Daten fertig sind, sollten Sie den Datenimportmodus deaktivieren, damit die automatischen Sicherungen und die Protokollierung für Ihre Datenbanken fortgesetzt werden können. Weitere Informationen finden Sie unter Importieren von Daten in Ihre MySQL-Datenbank und Importieren von Daten in Ihre PostgreSQL-Datenbank.

Wie greife ich auf die Daten in meiner von Lightsail verwalteten Datenbank zu?

Sie können sich mit Ihrer Datenbank verbinden und Ihre Daten mit jeder Standard-SQL-Clientanwendung abfragen. Wir empfehlen die MySQL Workbench für die GUI-basierte Administration und Abfrage. Sie finden die Verbindungsdaten auf der Datenbankverwaltungsseite für Ihre Datenbank (einschließlich der Endpunkt-URL und des DNS-Namens). Weitere Informationen finden Sie unter Connect zu Ihrer MySQL-Datenbank herstellen oder Verbindung zu Ihrer PostgreSQL-Datenbank herstellen in Amazon Lightsail.

Wie funktionieren von Lightsail verwaltete Datenbanken mit meinen Lightsail-Instances?

Nachdem Sie Ihre verwaltete Lightsail-Datenbank erstellt haben, können Sie sie sofort mit Ihrer Anwendung verwenden und Ihre Lightsail-Instanzen als Webserver oder andere dedizierte Workloads für Ihre App verwenden. Um Ihre Lightsail-Instanz mit einer Datenbank zu verbinden, verwenden Sie Ihren Datenbank-Endpunkt und verweisen Sie auf Ihr sicher gespeichertes Passwort, um die Datenbank als Ihren Datenspeicher im Code Ihrer Anwendung zu konfigurieren. Die Verbindungsdaten finden Sie auf den Datenbankverwaltungsseiten. Der Dateiname und der Speicherort für Ihre Datenbank-Konfigurationsdatei variieren je nach Anwendung. Beachten Sie, dass Sie mehrere Instances mit einer Datenbank verbinden können. Diese können dieselben oder andere Tabellen verwenden.

Wie kann ich die von Lightsail verwaltete Datenbank mit EC2-Instances verbinden, die in meinem Konto ausgeführt werden? AWS

Sie können Ihre von Lightsail verwaltete Datenbank mit EC2-Instances verbinden, indem Sie eine Verbindung über das öffentliche Internet herstellen. Beachten Sie, dass die Verbindung zu allen AWS Diensten Ihr Datenübertragungsvolumen in Anspruch nimmt und dass für Daten, die über das öffentliche Internet an AWS Dienste gesendet werden, die Ihr Datenübertragungsvolumen überschreiten, Überlastungsgebühren anfallen. Sie können kein VPC-Peering zwischen von Lightsail verwalteten Datenbanken und EC2-Instances verwenden.

Was ist der Unterschied zwischen öffentlichen und privaten Modi für meine von Lightsail verwaltete Datenbank?

Standardmäßig wird Ihre von Lightsail verwaltete Datenbank im privaten Modus erstellt, wodurch sie geschützt wird, indem nur Lightsail-Instanzen darauf zugreifen können. Sie können den öffentlichen Modus Ihrer Datenbank festlegen, wenn Sie eine Verbindung zu Software oder

Service über das öffentliche Internet herstellen müssen. Um die Sicherheit Ihrer Daten zu gewährleisten, empfehlen wir nicht, den öffentlichen Modus langfristig aktiviert zu halten. Sie können jederzeit über die Datenbankverwaltungsseiten zwischen dem öffentlichen und dem privaten Modus wechseln.

Kann ich die von meiner verwalteten Lightsail-Datenbank verwendeten Ports verwalten?

Nein, Lightsail verwaltet Ihre Ports aus Sicherheitsgründen automatisch und öffnet Port 3306 für MySQL für alle von Lightsail verwalteten Datenbanken im öffentlichen Modus. Wenn sich Ihre Datenbank im privaten Modus befindet, ist Ihre Datenbank nur für Ressourcen geöffnet, die in Ihrem Lightsail-Konto über das interne Netzwerk ausgeführt werden.

Unterstützen Lightsail-Dienste für verwaltete Datenbanken IPv6?

Von Lightsail verwaltete Datenbanken unterstützen IPv6 nicht.

Blockspeicher

Was kann ich mit Lightsail-Blockspeicher machen?

Der Lightsail-Blockspeicher bietet zusätzliche Speichervolumes (in Lightsail als „angeschlossene Festplatten“ bezeichnet), die Sie Ihrer Lightsail-Instanz zuordnen können, ähnlich wie bei einer einzelnen Festplatte. Angefügte Datenträger eignen sich für Anwendungen oder Software, die spezielle Daten von ihrem Kernservice trennen und Anwendungsdaten schützen müssen, sollte es zu einem Ausfall kommen oder andere Probleme mit Ihrer Instance oder Systemfestplatte auftreten. Angefügte Datenträger bieten Anwendungen und Software, die häufig auf ihre gespeicherten Daten zugreifen müssen, konsistente Leistung und geringe Latenz.

Lightsail-Blockspeicherfestplatten verwenden Solid-State-Laufwerke (SSD). Diese Art von Blockspeicher bietet ein ausgewogenes Verhältnis zwischen niedrigem Preis und guter Leistung und soll die überwiegende Mehrheit der Workloads unterstützen, die auf Lightsail ausgeführt werden. Für Kunden mit Anwendungen, die eine konstante IOPS-Leistung oder einen hohen Durchsatz pro Festplatte erfordern oder die große Datenbanken wie MongoDB, Cassandra usw. ausführen, empfehlen wir die Verwendung von Amazon EC2 mit GP2 oder Provisioned IOPS SSD-Speicher anstelle von Lightsail.

Wie unterscheiden sich angeschlossene Festplatten von dem Speicher, der in meinem Lightsail-Plan enthalten ist?

Die in Ihrem Lightsail-Plan enthaltene Systemfestplatte ist das Root-Gerät Ihrer Instanz. Wenn Sie Ihre Instance beenden, wird auch die Systemfestplatte beendet. Bei einem Instance-

Ausfall, kann auch die Systemfestplatte beeinträchtigt werden. Sie können die Systemfestplatte zudem auch weder von Ihrer Instance trennen noch sie getrennt sichern. Daten, die auf einem angefügten Datenträger gespeichert sind, bleiben unabhängig von der Instance erhalten. Angefügte Datenträger können getrennt und zwischen Instances verschoben werden. Sie können unabhängig von einer Instance gesichert werden, indem Sie einen manuellen Snapshot des Datenträgers erstellen. Um Ihre Daten zu schützen, empfehlen wir, die Systemfestplatte Ihrer Lightsail-Instanz nur für temporäre Daten zu verwenden. Für Daten, die eine höhere Dauerhaftigkeit erfordern, empfehlen wir die Verwendung angefügter Datenträger und eine regelmäßige Sicherung des Datenträgers mithilfe von Datenträger- oder Instance-Snapshots.

Wie groß kann der angefügte Datenträger sein?

Jede angeschlossene Festplatte kann bis zu 16 TB groß sein, und die Gesamtmenge des angehängten Blockspeichers in einem Lightsail-Konto darf 20 TB nicht überschreiten.

Wie viele Festplatten kann ich pro Lightsail-Instanz anhängen?

Sie können bis zu 15 Festplatten an eine Lightsail-Instanz anschließen.

Kann ich einen Datenträger an mehr als eine Instance anfügen?

Nein, Datenträger können nur einer Instance gleichzeitig angefügt werden.

Muss mein Datenträger einer Instance angefügt werden?

Nein, Sie müssen Ihren Datenträger keiner Instance anfügen. Der Datenträger kann in einem nicht zugewiesenen Status in Ihrem Konto verbleiben. Die Tatsache, dass Ihr Datenträger keiner Instance angefügt ist, wirkt sich nicht auf den Preis aus.

Kann ich die Größe meines angefügten Datenträgers ändern?

Ja, Sie können die Größe des Datenträgers erweitern. Nehmen Sie dazu einen Datenträger-Snapshot und erstellen Sie mithilfe dieses Snapshots einen neuen, größeren Datenträger.

Bietet Lightsail Block Storage Verschlüsselung?

Ja, um Ihre Daten zu schützen, werden alle mit Lightsail verbundenen Festplatten und Festplatten-Snapshots standardmäßig im Ruhezustand verschlüsselt, wobei Schlüssel verwendet werden, die Lightsail in Ihrem Namen verwaltet. Lightsail bietet auch die Verschlüsselung von Daten, wenn sie zwischen Lightsail-Instanzen und angeschlossenen Festplatten übertragen werden.

Welche Verfügbarkeit kann ich von Lightsail Block Storage erwarten?

Der Lightsail-Blockspeicher ist so konzipiert, dass er hochverfügbar und zuverlässig ist. Jeder angefügte Datenträger wird in seiner Availability Zone automatisch repliziert, um Schutz bei Ausfall von Komponenten zu bieten. Lightsail-Blockspeicherfestplatten sind für eine Verfügbarkeit von 99,99% konzipiert. Lightsail unterstützt auch Festplatten-Snapshots, um regelmäßige Backups Ihrer Daten zu ermöglichen.

Wie kann ich meinen angefügten Datenträger sichern?

Sie können Ihren Datenträger sichern, indem Sie einen manuellen Snapshot des Datenträgers erstellen. Sie können auch Ihre gesamte Instance und alle angefügten Datenträger sichern, indem Sie einen manuellen Snapshot der Instance erstellen,oder indem Sie automatische Snapshots für die Instance mit dem angefügten Datenträger aktivieren. An Instances angefügte Datenträger sind in den manuellen und automatischen Snapshots der Instance enthalten.

Load Balancer

Was kann ich mit Lightsail-Loadbalancern machen?

Mit Lightsail Load Balancers können Sie hochverfügbare Websites und Anwendungen erstellen. Lightsail-Loadbalancer verteilen den Traffic auf Instances in verschiedenen Availability Zones und leiten den Traffic nur auf fehlerfreie Ziel-Instances weiter. Dadurch wird das Risiko verringert, dass Ihre Anwendung aufgrund eines Problems mit Ihrer Instance oder eines Rechenzentrumsausfalls ausfällt. Mit Lightsail-Loadbalancern und mehreren Zielinstanzen kann Ihre Website oder Anwendung auch dem Anstieg des Web-Traffics Rechnung tragen und eine gute Leistung für Ihre Besucher zu Spitzenlastzeiten aufrechterhalten.

Darüber hinaus können Sie Lightsail-Load Balancer verwenden, um sichere Anwendungen zu erstellen und HTTPS-Verkehr zu akzeptieren. Lightsail vereinfacht das Anfordern, Bereitstellen und Verwalten von SSL/TLS-Zertifikaten. Die integrierte Zertifikatverwaltung fordert in Ihrem Namen Zertifikate an, erneuert diese und fügt sie automatisch Ihrer Load Balancer hinzu.

Kann ich Load Balancer mit Instances in verschiedenen s oder verschiedenen AWS-Region Availability Zones verwenden?

Sie können Load Balancer nicht mit Instances verwenden, die in verschiedenen AWS-Region s ausgeführt werden. Jedoch können Sie Ziel-Instances mit Ihrer Load Balancer über verschiedene Availability Zones hinweg verwenden. Wir empfehlen Ihnen sogar, Ihre Ziel-Instances über

mehrere Availability Zones hinweg zu verteilen, um so die Verfügbarkeit Ihrer Anwendung zu optimieren.

Wie geht mein Lightsail Load Balancer mit Verkehrsspitzen um?

Lightsail Load Balancer skalieren automatisch, um Traffic-Spitzen in Ihrer Anwendung zu bewältigen, ohne dass Sie sie manuell anpassen müssen. Wenn bei Ihrer Anwendung ein vorübergehender Anstieg des Datenverkehrs auftritt, skaliert Ihr Lightsail-Load Balancer automatisch und leitet den Datenverkehr weiterhin effizient an Ihre Lightsail-Instances weiter. Ihr Lightsail Load Balancer ist zwar so konzipiert, dass er Datenverkehrsspitzen problemlos bewältigen kann, bei Anwendungen, bei denen ständig ein sehr hohes Datenvolumen auftritt, kann es jedoch zu Leistungseinbußen oder Drosselungen kommen. Wenn Sie damit rechnen, dass Ihre Anwendung regelmäßig mehr als 5 GB/Stunde an Daten verwalten oder regelmäßig über eine große Anzahl an Verbindungen verfügen wird (>400k neue Verbindungen/Stunde, >15k aktive, gleichzeitige Verbindungen), empfehlen wir stattdessen die Verwendung von Amazon-EC2-Anwendungs-Load-Balancer.

Wie leiten Lightsail-Loadbalancer den Traffic an meine Ziel-Instances weiter?

Lightsail Load Balancer leiten den Traffic auf der Grundlage eines Round-Robin-Algorithmus an Ihre fehlerfreien Ziel-Instances weiter.

Woher weiß Lightsail, ob meine Ziel-Instances fehlerfrei sind?

Nachdem Sie Ihren Load Balancer erstellt und Ihre Instances angehängt haben, sendet Lightsail eine Health Check-Anfrage an das Stammverzeichnis Ihrer Webanwendung. Sie können den Speicherort anpassen, indem Sie einen Pfad (eine allgemeine Datei- oder Webseiten-URL) angeben, an den Lightsail pingt. Wenn die Zielinstanz über diesen Pfad erreicht werden kann, leitet Lightsail den Verkehr dorthin weiter. Wenn eine Ihrer Ziel-Instances nicht reagiert, schlägt die Zustandsprüfung fehl und Lightsail leitet keinen Traffic an diese Instance weiter. Weitere Informationen über die Zustandsprüfungen

Wie viele Instances kann ich dem Load Balancer anfügen?

Sie können Ihrem Load Balancer so viele Ziel-Instances hinzufügen, wie Sie möchten — bis zu Ihrem Instance-Kontingent für Lightsail-Konten.

Kann ich eine Instance mehreren Load Balancer zuweisen?

Ja, Lightsail unterstützt das Hinzufügen von Instances als Ziel-Instances für mehr als einen Load Balancer, falls gewünscht.

Was passiert mit meinen Ziel-Instances, wenn ich meinen Load Balancer lösche?

Wenn Sie Ihren Load Balancer löschen, werden die angehängten Ziel-Instances weiterhin normal ausgeführt und in der Lightsail-Konsole als reguläre Lightsail-Instances angezeigt. Beachten Sie, dass Sie Ihre DNS-Datensätze wahrscheinlich aktualisieren müssen, um den Datenverkehr nach dem Löschen des Load Balancers an eine Ihrer vorherigen Ziel-Instances weiterzuleiten.

Was ist Sitzungspersistenz?

Anhand der Sitzungspersistenz kann der Load Balancer die Sitzung eines Besuchers an eine bestimmte Ziel-Instance binden. So wird sichergestellt, dass alle Anforderungen, die während der Sitzung vom Benutzer gesendet werden, an dieselbe Ziel-Instance weitergeleitet werden. Lightsail unterstützt Sitzungspersistenz für Anwendungen, bei denen Besucher aus Gründen der Datenkonsistenz dieselben Zielinstanzen aufrufen müssen. So profitieren beispielsweise viele Anwendungen, die eine Benutzer-Authentifizierung erfordern, von der Sitzungspersistenz. Sie können die Sitzungspersistenz für bestimmte Load Balancer nach der Erstellung auf den Verwaltungsbildschirmen für den Load Balancer aktivieren. Weitere Informationen finden Sie unter Aktivieren der Sitzungspersistenz für einen Load Balancer.

Welche Verbindungen unterstützen Lightsail Load Balancer?

Lightsail Load Balancer unterstützen HTTP- und HTTPS-Verbindungen.

Unterstützen Lightsail-Loadbalancer IPv6?

Lightsail-Loadbalancer, die nach dem 12. Januar 2021 erstellt wurden, arbeiten standardmäßig im Dual-Stack-Modus (d. h. sie akzeptieren Client-Verkehr sowohl über das IPv4- als auch über das IPv6-Protokoll). IPv6 kann auf Load Balancer aktiviert werden, die vor diesem Datum erstellt wurden, über einen Schalter auf der Registerkarte Netzwerk der Verwaltungsseite des Load Balancers. IPv6 kann auch auf jeden Load Balancer mit diesem Schalter deaktiviert werden.

Müssen die Instances hinter einem Load Balancer IPv6-aktiviert sein, um den Load Balancer zu verwenden, die IPv6-aktiviert ist?

Nein. Load Balancer akzeptieren sowohl IPv4- als auch IPv6-Datenverkehr und wandeln ihn nahtlos in IPv4 um, wenn sie mit den Instances im Backend kommunizieren. Instances hinter eines Load Balancers können daher entweder Dual-Stack oder nur IPv4 sein.

Netzwerkverteilungen für die Bereitstellung von Inhalten

Was kann ich mit Lightsail CDN-Distributionen machen?

Mithilfe von Lightsail Content Delivery Network (CDN) -Distributionen können Sie die Bereitstellung von Inhalten, die auf Ihren Lightsail-Ressourcen gehostet werden, auf einfache Weise beschleunigen, indem Sie sie im globalen Bereitstellungsnetzwerk von Amazon speichern und bereitstellen, das von Amazon betrieben wird. CloudFront Verteilungen helfen Ihnen auch, dass Ihre Website HTTPS-Datenverkehr unterstützt, indem sie einfache Erstellung und Hosting von SSL-Zertifikaten bereitstellen. Schließlich können Distributionen dazu beitragen, die Belastung Ihrer Lightsail-Ressourcen zu reduzieren und Ihrer Website dabei zu helfen, große Traffic-Spitzen zu bewältigen. Wie bei allen Funktionen von Lightsail kann die Einrichtung mit nur wenigen Klicks abgeschlossen werden, und Sie zahlen einen einfachen monatlichen Preis.

Welche Arten von Ressourcen kann ich als Ursprungsserver meiner Verteilung verwenden?

Lightsail-Distributionen ermöglichen es Ihnen, Ihre Lightsail-Instances und Load Balancer als Ursprünge zu verwenden. Lightsail-Container werden derzeit nicht als Origins unterstützt. Ressourcen außerhalb von Lightsail, wie z. B. S3-Buckets, werden nicht unterstützt.

Muss ich eine statische IPv4-Adresse an meine Lightsail-Instance anhängen, um sie als Ursprung für meine Lightsail-Distribution zu verwenden?

Ja, statische IPv4-Adressen müssen Instances angefügt werden, die als Ursprungsserver angegeben sind. Lightsail-Distributionen unterstützen IPv6 derzeit nicht.

Wie richte ich eine Lightsail-Distribution mit meiner WordPress Website ein?

Erstellen Sie Ihre Distribution, wählen Sie Ihre WordPress Instance als Origin aus, wählen Sie Ihren Plan und schon sind Sie fertig. Lightsail-Distributionen konfigurieren Ihre Distributionseinstellungen automatisch, um die Leistung für die meisten Konfigurationen zu optimieren. WordPress

Kann ich mehrere Ursprünge anfügen?

Sie können zwar nicht mehrere Ursprünge an Ihre Lightsail-Distribution anhängen, Sie können jedoch mehrere Instances an einen Lightsail-Load Balancer anhängen und ihn als Ursprung Ihrer Distribution angeben.

Unterstützen Lightsail-Distributionen die Erstellung von Zertifikaten?

Ja. Mit Lightsail Distributionen können Sie Zertifikate ganz einfach direkt von der Verwaltungsseite Ihrer Distribution aus erstellen, überprüfen und anhängen.

Ist ein Zertifikat erforderlich?

Ein Zertifikat ist nur erforderlich, wenn Sie Ihren benutzerdefinierten Domänennamen mit Ihrer Verteilung verwenden möchten. Alle Lightsail-Distributionen werden mit einem eindeutigen CloudFront Amazon-Domainnamen erstellt, der HTTPS-fähig ist. Wenn Sie jedoch Ihre benutzerdefinierte Domäne mit Ihrer Verteilung verwenden möchten, müssen Sie ein Zertifikat für Ihre benutzerdefinierte Domäne an Ihre Verteilung anhängen.

Ist die Anzahl der Zertifikate, die ich erstellen kann, begrenzt?

Ja, weitere Informationen finden Sie in den Lightsail-Servicekontingenten.

Wie kann ich meine Verteilung so konfigurieren, dass HTTP-Anfragen an HTTPS umgeleitet werden?

Lightsail-Distributionen leiten alle HTTP-Anfragen automatisch an HTTPS weiter, um sicherzustellen, dass Ihre Inhalte sicher bereitgestellt werden.

Wie kann ich meine Apex-Domain so konfigurieren, dass sie auf meine Lightsail-Distribution verweist?

Um Ihre Apex-Domäne auf Ihre CDN-Verteilung zu verweisen, müssen Sie im Domain Name System (DNS) Ihrer Domäne eine ALIAS-Akte erstellen, die Ihre Apex-Domäne der Standarddomäne Ihrer Verteilung zuordnet. Wenn Ihr DNS-Hosting-Anbieter keine ALIAS-Einträge unterstützt, können Sie Lightsail-DNS-Zonen verwenden, um Ihre Apex-Domain einfach so zu konfigurieren, dass sie auf die Domain Ihrer Distribution verweist.

Was sind die Unterschiede zwischen den Instanzdatenübertragungskontingenten von Lightsail und den Datenübertragungsquoten für Distributionen?

Während die Datenübertragung IN und AUS für das Datenübertragungskontingent Ihrer Instance angerechnet wird, zählt nur die Datenübertragung AUS zu Ihrem Ursprungsserver und zu Ihren Viewern für das Kontingent Ihrer Verteilung. Darüber hinaus wird für jede Datenübertragung AUS, die über das Kontingent Ihrer Verteilung hinausgeht, eine Überschreitungsgebühr erhoben, während einige Arten der Datenübertragung AUS für Instances kostenlos sind. Schließlich verwenden Lightsail-Distributionen ein anderes regionales Deckungsmodell, obwohl die meisten Tarife denen entsprechen, die beispielsweise bei Überschreitung berechnet werden.

Kann ich den Plan ändern, der mit meiner Verteilung verknüpft ist?

Ja, Sie können Ihren Verteilungsplan einmal im Monat ändern. Wenn Sie Ihren Plan ein zweites Mal ändern möchten, müssen Sie bis zum Anfang des Folgemonats warten, um dies zu tun.

Woher weiß ich, dass meine Verteilung funktioniert?

Lightsail-Verteilungen bieten Ihnen eine Vielzahl von Metriken, mit denen Sie die Leistung Ihrer Distribution verfolgen können, darunter die Gesamtzahl der Anfragen, die Ihr Vertrieb erhalten hat, die Datenmenge, die Ihre Distribution an Kunden und an Ihre Herkunft gesendet hat, sowie den Prozentsatz der Anfragen, die zu Fehlern geführt haben. Darüber hinaus können Sie Warnungen erstellen, die mit Verteilungsmetriken verknüpft sind.

Kann ich zwischengespeicherte Inhalte in meiner Lightsail-Distribution löschen?

Sie können alle zwischengespeicherten Inhalte löschen, jedoch nicht bestimmte Dateien oder Ordner.

Wann sollte ich Lightsail-Distributionen anstelle von Amazon-Distributionen verwenden? CloudFront

Lightsail-Distributionen wurden speziell für Benutzer entwickelt, die Websites oder Webanwendungen auf Lightsail-Ressourcen wie Instances und Load Balancern hosten. Wenn Sie einen anderen Dienst AWS zum Hosten Ihrer Website oder App verwenden, komplexe Konfigurationsanforderungen haben oder eine Arbeitslast haben, die eine hohe Anzahl von Anfragen pro Sekunde oder eine große Menge an Videostreaming beinhaltet, empfehlen wir Ihnen, Amazon zu verwenden CloudFront.

Kann ich meinen Vertrieb über das Lightsail Content Delivery Network (CDN) zu Amazon verlagern? CloudFront

Ja, Sie können Ihre Lightsail-Distribution verschieben, indem Sie eine ähnlich konfigurierte Distribution in Amazon erstellen. CloudFront Alle Einstellungen, die in einer Lightsail-Distribution konfiguriert werden können, können auch in einer CloudFront Distribution konfiguriert werden. Gehen Sie wie folgt vor, um Ihre Distribution zu verschieben: CloudFront

- Erstellen Sie einen Snapshot Ihrer Lightsail-Instanz, die als Ursprung Ihrer Distribution konfiguriert ist. Exportieren Sie den Snapshot in Amazon EC2, und erstellen Sie dann eine neue Instance aus dem Snapshot in EC2. Weitere Informationen finden Sie unter Exportieren von Snapshots nach Amazon EC2.

  > **Note**
  >
  > Erstellen Sie in Elastic Load Balancing eine Application Load Balancer, wenn Sie einen Load Balancer für Ihre Website oder Webanwendung vornehmen müssen. Weitere Informationen finden Sie im Elastic Load Balancing-Benutzerhandbuch.

- Deaktivieren Sie benutzerdefinierte Domänen für Ihre Lightsail-Distribution, um Zertifikate zu trennen, die Sie möglicherweise an sie angehängt haben. Weitere Informationen finden Sie unter Deaktivieren benutzerdefinierter Domains für Ihre Amazon Lightsail-Distributionen.
- Führen Sie mit AWS Command Line Interface (AWS CLI) den Befehl get-distributions aus, um eine Liste der Einstellungen Ihrer Lightsail-Distribution abzurufen. Weitere Informationen finden Sie unter get-distributions in der AWS CLI -Referenz.
- Melden Sie sich bei der CloudFrontKonsole an und erstellen Sie eine Distribution mit denselben Konfigurationseinstellungen wie Ihre Lightsail-Distribution. Weitere Informationen finden Sie unter Creating a Distribution im Amazon CloudFront Developer Guide.
- Erstellen Sie ein Zertifikat in AWS Certificate Manager c (ACM), das Sie Ihrer CloudFront Distribution beifügen werden. Weitere Informationen finden Sie unter Anfordern eines öffentliches Zertifikats im ACM-Benutzerhandbuch.
- Aktualisieren Sie Ihre CloudFront Distribution, sodass sie das von Ihnen erstellte ACM-Zertifikat verwendet. Weitere Informationen finden Sie im CloudFront Benutzerhandbuch unter Aktualisieren Ihrer CloudFront Distribution.

Wie soll Lightsail CDN verwendet werden?

Lightsail-CDN-Distributionen werden mithilfe von Datenübertragungspaketen zu festen Preisen erstellt, um die Kosten für die Nutzung des Dienstes einfach und vorhersehbar zu machen. Verteilungsbündel sind so konzipiert, dass sie die Nutzung eines Monats abdecken. Die Verwendung von Verteilungbündel in einer Weise, um zu vermeiden, dass Überschreitungsgebühren entstehen (einschließlich, aber nicht beschränkt auf, häufige Upgrades oder Downgrades von Bündeln oder die Verwendung einer übermäßig großen Anzahl von Verteilungen mit einem einzigen Ursprungsserver), ist über den beabsichtigten Verwendungsbereich hinaus und ist nicht zulässig. Darüber hinaus sind Workloads, die eine hohe Anzahl von Anfragen pro Sekunde oder eine große Menge an Video streaming beinhalten, nicht zulässig. Diese Verhaltensweisen können zu einer Drosselung oder Sperrung Ihrer Datendienste oder Ihres Kontos führen.

Unterstützen Lightsail CDN-Verteilungen IPv6?

Für alle Lightsail-CDN-Verteilungen ist IPv6 standardmäßig aktiviert. Die Hostnamen der Verteilung werden in IPv4- und IPv6-Adressen aufgelöst. IPv6 kann über einen Schalter auf der Netzwerk-Registerkarte auf der CDN-Verwaltungsseite deaktiviert werden.

Müssen die Ursprungsserver IPv6-aktiviert sein, um mit den Lightsail-CDN-Verteilungen funktionieren zu können?

Nein. CDN-Verteilungen akzeptieren sowohl IPv6- als auch IPv4-Datenverkehr und wandeln ihn nahtlos in IPv4 um, wenn sie mit den Ursprungsservern im Backend kommunizieren. Instances hinter einer Verteilung können daher entweder Dual-Stack oder nur IPv4 sein.

Zertifikate

Wie kann ich von Lightsail bereitgestellte Zertifikate verwenden?

SSL/TLS-Zertifikate werden verwendet, um die Identität Ihrer Website oder Anwendung nachzuweisen und die Verbindung zwischen Browsern und Ihrer Website zu schützen. Lightsail stellt ein signiertes Zertifikat zur Verwendung mit Ihrem Load Balancer bereit, und der Load Balancer ermöglicht die SSL/TLS-Terminierung, bevor verifizierter Datenverkehr über das sichere Netzwerk an Ihre Ziel-Instances weitergeleitet wird. AWS Lightsail-Zertifikate können nur mit Lightsail-Load Balancern verwendet werden, nicht mit einzelnen Lightsail-Instances.

Wie validiere ich mein Zertifikat?

Lightsail-Zertifikate sind domänenvalidiert, was bedeutet, dass Sie einen Identitätsnachweis erbringen müssen, indem Sie bestätigen, dass Sie Eigentümer der Domain Ihrer Website sind oder Zugriff darauf haben, bevor das Zertifikat von der Zertifizierungsstelle bereitgestellt werden kann. Wenn Sie ein neues Zertifikat anfordern, versucht Lightsail, das Zertifikat automatisch zu validieren. Wenn das Zertifikat nicht automatisch validiert werden kann, fordert Lightsail Sie auf, der oder den DNS-Zone (n) der Domain (n), die Sie validieren, einen CNAME-Eintrag hinzuzufügen. Sie haben 72 Stunden Zeit, um den CNAME-Eintrag dort hinzuzufügen, wo Sie derzeit Ihre DNS-Zonen verwalten — entweder Lightsail DNS-Management oder ein externer DNS-Hosting-Anbieter.

Was passiert, wenn ich meine Domäne nicht validieren kann?

Sie müssen aus Sicherheitsgründen validieren, dass Sie der Besitzer einer Domäne sind. Das heißt, wenn Sie oder jemand in Ihrer Organisation aus irgendeinem Grund keinen DNS-Eintrag zur Validierung Ihres Zertifikats hinzufügen kann, können Sie keinen HTTPS-fähigen Load Balancer mit Lightsail verwenden.

Wie viele Domänen und Unterdomänen kann ich meinem Zertifikat hinzufügen?

Sie können pro Zertifikat bis zu 10 Domains oder Unterdomains hinzufügen. Lightsail unterstützt derzeit keine Wildcard-Domains.

Wie kann ich die Domänen ändern, die meinem Zertifikat zugewiesen sind?

Um die Domänen, die Ihrem Zertifikat zugewiesen sind, zu ändern (hinzuzufügen/zu löschen), müssen Sie das Zertifikat erneut einreichen und sich nochmals als Eigentümer der Domäne(n) ausweisen. Befolgen Sie die Schritte auf den Bildschirmen für die Zertifikatsverwaltung, um Ihr Zertifikat zu generieren und nach Aufforderung Domänen hinzuzufügen oder zu entfernen.

Wie erneuere ich mein Zertifikat?

Lightsail bietet eine verwaltete Verlängerung Ihrer SSL/TLS-Zertifikate. Das bedeutet, dass Lightsail versucht, die Zertifikate automatisch zu verlängern, bevor sie ablaufen, ohne dass Sie etwas unternehmen müssen. Ihr Lightsail-Zertifikat muss aktiv mit einem Load Balancer verknüpft sein, bevor es automatisch erneuert werden kann.

Was passiert mit meinen Zertifikat, wenn ich meinen Load Balancer lösche?

Wenn Ihr Load Balancer gelöscht wird, wird auch Ihr Zertifikat gelöscht. Wenn Sie für die gleichen Domäne(n) zu einem späteren Zeitpunkt ein Zertifikat benötigen, müssen Sie ein neues Zertifikat anfordern und validieren.

Kann ich mein von Lightsail bereitgestelltes Zertifikat herunterladen?

Nein, Lightsail-Zertifikate sind an Ihr Lightsail-Konto gebunden und können nicht entfernt und außerhalb von Lightsail verwendet werden.

Manuelle und automatische Snapshots

Was sind Snapshots?

Snapshots sind point-in-time Backups von Instanzen, Datenbanken oder Blockspeicherfestplatten. Sie können jederzeit einen Snapshot Ihrer Ressourcen erstellen oder automatische Snapshots auf Instanzen und Festplatten aktivieren, damit Lightsail Snapshots für Sie erstellt. Sie können Snapshots als Baselines verwenden, um neue Ressourcen zu erstellen oder Ihre Daten zu sichern. Ein Snapshot enthält alle Daten, die erforderlich sind, um Ihre Ressource wiederherzustellen (ab dem Zeitpunkt, an dem der Snapshot erstellt wurde). Wenn Sie eine Ressource basierend auf einem Snapshot wiederherstellen, startet die neue Ressource als exakte Kopie der ursprünglichen Ressource, die zum Erstellen des Snapshots verwendet wurde.

Sie können manuell Snapshots Ihrer Lightsail-Instanzen, Festplatten und Datenbanken erstellen, oder Sie können automatische Snapshots verwenden, um Lightsail anzuweisen, täglich

automatisch Snapshots Ihrer Instanzen und Festplatten zu erstellen. Weitere Informationen finden Sie unter Snapshots.

Was sind automatische Snapshots?

Automatische Snapshots sind eine Möglichkeit, tägliche Snapshots Ihrer Linux/Unix-Instances in Amazon Lightsail zu planen. Sie können eine Tageszeit auswählen, und Lightsail erstellt automatisch an jedem Tag zu der von Ihnen gewählten Uhrzeit einen Snapshot für Sie und behält immer Ihre sieben neuesten automatischen Schnappschüsse bei. Das Aktivieren von Snapshots ist kostenlos – Sie zahlen nur für den tatsächlichen Speicher, der von Ihren Snapshots verwendet wird.

Was sind die Unterschiede zwischen manuellen und automatischen Snapshots?

Automatische Snapshots können nicht direkt markiert oder direkt in Amazon EC2 exportiert werden. Automatische Snapshots können jedoch kopiert und in manuelle Snapshots konvertiert werden. Um einen automatischen Snapshot in einen manuellen Snapshot zu kopieren, wählen Sie im Kontextmenü des automatischen Snapshots die Option Beibehalten aus, um ihn als manuellen Snapshot zu kopieren.

Welche Ressourcen unterstützen Snapshots?

Manuelle Snapshots können für Instances, Datenbanken und Datenträger erstellt werden.

Automatische Snapshots können für Linux- oder Unix-Instances mithilfe der Lightsail-Konsole, der Lightsail-API oder und für Festplatten, die nur die Lightsail-API verwenden AWS CLI, oder aktiviert werden. AWS CLI Automatische Snapshots werden derzeit für Windows-Instances oder verwaltete Datenbanken nicht unterstützt.

Wie lange kann ich Snapshots speichern?

Manuelle Snapshots werden so lange gespeichert, bis Sie sie löschen. Weitere Informationen finden Sie unter Löschen von Schnappschüssen in Amazon Lightsail.

Automatische Snapshots werden gespeichert, bis sie durch neuere automatische Snapshots ersetzt werden. Lightsail speichert die letzten sieben automatischen Snapshots, bevor der älteste gelöscht und durch den neuesten ersetzt wird. Sie können jedoch einen bestimmten automatischen Snapshot aufbewahren, indem Sie ihn als manuellen Snapshot kopieren. Weitere Informationen finden Sie unter Automatische Snapshots von Instances oder Festplatten in Amazon Lightsail aufbewahren. Ihnen wird die Snapshot-Speichergebühr für die automatischen Snapshots in Ihrem Konto in Rechnung gestellt.

Wie werden automatische Snapshots aktiviert?

Automatische Snapshots können mithilfe der Lightsail-Konsole, der Lightsail-API oder AWS CLI beim Erstellen einer Linux- oder Unix-Instance oder später, nachdem die Instanz ausgeführt wird, aktiviert werden.

Automatische Snapshots können auch für Festplatten aktiviert werden, wenn Sie sie erstellen oder nachdem sie erstellt wurden. Dies ist jedoch nur mit der Lightsail-API oder der AWS-CLI möglich.

Weitere Informationen finden Sie unter Automatische Snapshots für Instances oder Festplatten in Amazon Lightsail aktivieren oder deaktivieren.

Wann werden automatische Snapshots erstellt?

Wenn Sie automatische Snapshots aktivieren, wird, basierend auf der AWS-Region , in der sich die Ressource befindet, eine Standardzeit festgelegt. Sie können den automatischen Snapshot in stündlichen Schritten auf Ihre bevorzugte Tageszeit ändern. Weitere Informationen finden Sie unter Ändern der automatischen Snapshot-Zeit für Instances oder Festplatten in Amazon Lightsail.

Wie viele Snapshots kann ich speichern?

Sie können beliebig viele manuelle Snapshots speichern. Es werden jedoch nur die neuesten sieben automatischen Snapshots gespeichert, bevor der älteste durch den neuesten ersetzt wird.

Wie werden Snapshots in Rechnung gestellt?

Sie zahlen nur für die Schnappschüsse, die auf Ihrem Lightsail-Konto gespeichert sind. Die Speicherung von Lightsail-Snapshots (manuell und automatisch) kostet 0,05 USD/GB pro Monat.

Gehen meine Snapshots verloren, wenn ich automatische Snapshots deaktiviere?

Nein. Wenn Sie automatische Schnappschüsse deaktivieren, erstellt Lightsail keine täglichen Schnappschüsse mehr und Ihre vorhandenen automatischen Schnappschüsse werden beibehalten. Wenn Sie automatische Schnappschüsse wieder aktivieren, nimmt Lightsail weiterhin tägliche Schnappschüsse auf, löscht den ältesten und ersetzt ihn durch den neuesten.

Was soll ich tun, wenn ich nicht möchte, dass ein automatischer Snapshot ersetzt wird?

Sie können einen bestimmten automatischen Snapshot aufbewahren, indem Sie ihn als manuellen Snapshot kopieren. Weitere Informationen finden Sie unter Automatische Snapshots von Instances oder Festplatten in Amazon Lightsail aufbewahren.

Kann ich einen automatischen Snapshot löschen?

Sie können einen automatischen Snapshot jederzeit löschen, indem Sie Delete (Löschen) im Kontextmenü des automatischen Snapshots auswählen. Weitere Informationen finden Sie unter Löschen automatischer Instance-Snapshots.

Wie kann ich Snapshots verwenden?

Snapshots können als Basis verwendet werden oder um neue Ressourcen zu erstellen, wenn ein Problem mit der ursprünglichen Ressource aufgetreten ist. Snapshots können auch Weitere Informationen finden Sie unter Snapshots.

Snapshots können auch in Amazon EC2 exportiert werden, um neue Ressourcen innerhalb dieses Service zu erstellen. Weitere Informationen finden Sie unter Exportieren von Snapshots nach Amazon EC2.

Netzwerk

Wie verwende ich IPs in Lightsail?

Jede Lightsail-Instance erhält automatisch eine private IPv4-Adresse, eine öffentliche IPv4-Adresse oder eine öffentliche IPv6-Adresse (IPv6 muss für Instances, die vor dem 12. Januar 2021 erstellt wurden, manuell aktiviert werden). Sie können die private IP verwenden, um Daten zwischen Lightsail-Instanzen und AWS Ressourcen privat und kostenlos zu übertragen. Sie können die öffentliche IP zum Verbinden Ihrer Instance mit dem Internet nutzen, z. B. über eine registrierte Domäne oder über eine SSH- oder RDP-Verbindung von Ihrem Computer vor Ort. Sie können der Instance außerdem eine statische IPv4-Adresse zuweisen, welche die öffentliche IPv4-Adresse durch eine IPv4-Adresse ersetzt, die sich auch beim Anhalten oder Starten der Instance nicht ändert. Die der Instance zugewiesenen IPv6-Adressen bleiben unverändert, bis die Instance gelöscht wird oder die IPv6-Adresse manuell freigegeben wird, indem IPv6 auf der Instance deaktiviert wird.

Unterstützt Lightsail reine IPv6-Instances?

Ja, Lightsail-Instances unterstützen Dual-Stack-Konfigurationen (IPv4 und IPv6) und reine IPv6-Konfigurationen.

Was ist eine statische IP?

Eine statische IP ist eine feste, öffentliche IP, die Ihrem Lightsail-Konto zugewiesen ist. Sie können einer Instance eine statische IPv4-Adresse zuweisen, die ihre öffentliche IPv4 ersetzt.

Wenn Sie entscheiden, Ihre Instance durch eine andere zu ersetzen, können Sie die statische IP der neuen Instance zuweisen. Auf diese Weise müssen Sie nicht alle externen Systeme neu konfigurieren (z. B. DNS-Datensätze), um immer auf eine neue IP-Adresse zu verweisen, wenn Sie Ihre Instance ersetzen möchten. Lightsail unterstützt derzeit nur statische IPs für IPv4. Statische IPv6-Adressen sind nicht verfügbar. IPv6-Adressen, die der Instance zugewiesen sind, bleiben jedoch unverändert, bis die Instance gelöscht wird oder die IPv6-Adresse manuell freigegeben wird, indem IPv6 für die Instance deaktiviert wird.

Wie viele statische IPs kann ich an eine Instance anhängen?

Sie können eine statische IP an eine Instance anhängen.

Was sind DNS-Datensätze?

DNS ist ein weltweit verteilter Service, der vom Menschen lesbare Namen, wie beispielsweise `www.example.com`, in alphanumerische IP-Adressen wie `192.0.2.1` umwandelt, die zur Verbindung zwischen Computern verwendet werden. Mit Lightsail können Sie Ihre registrierten Domainnamen ganz einfach den öffentlichen IP-Adressen Ihrer Lightsail-Instanzen zuordnen. `photos.example.com` Auf diese Weise übersetzt Lightsail die Adresse automatisch `example.com` in die IP der Instanz, zu der Sie Ihre Benutzer weiterleiten möchten, wenn sie menschenlesbare Namen wie in ihren Browser eingeben. Jede dieser Übersetzungen wird als DNS-Abfrage bezeichnet.

Es ist wichtig zu wissen, dass Sie eine Domain zunächst registrieren müssen, um sie in Lightsail verwenden zu können. Sie können Domains mit Lightsail oder Ihrem bevorzugten DNS-Registrar registrieren.

Kann ich Firewall-Einstellungen für meine Instance verwalten?

Ja. Sie können den Datenverkehr für Ihre Instances mithilfe der Lightsail-Firewall steuern. In der Lightsail-Konsole können Sie Regeln festlegen, welche Ports Ihrer Instance für verschiedene Arten von Traffic öffentlich zugänglich sind.

Domains

Was kann ich mit Lightsail-Domains machen?

Mit Lightsail-Domains können Sie Domains für Ihre Website oder Anwendung registrieren und verwalten. Wenn Sie Domains haben, die bei anderen Anbietern registriert sind, können Sie die Verwaltung dieser Domains an Lightsail übertragen. Sie können diese Domains auch auf Ihre Lightsail-Ressourcen verweisen.

Welche Top-Level-Domänen (TLDs) kann ich verwenden?

Lightsail verwendet dieselben generischen TLDs wie Amazon Route 53 Wenn Sie eine geografische Domain registrieren möchten, empfehlen wir Ihnen, die Route-53-Konsole zu verwenden. Ihre geografische Domain ist in der Lightsail-Konsole verfügbar, nachdem sie über Route 53 registriert wurde. Weitere Informationen zu den TLDs, die Lightsail unterstützt, finden Sie im Amazon Route 53 Developer Guide unter Domains, die Sie bei Amazon Route 53 registrieren können.

Kann ich Lightsail zum DNS-Dienst für meine bestehende Domain machen?

Sie können die DNS-Verwaltung einer Domain, die Sie mit einem anderen DNS-Dienstanbieter registriert haben, an Lightsail übertragen. Weitere Informationen finden Sie unter Erstellen einer DNS-Zone zur Verwaltung der DNS-Datensätze Ihrer Domain.

Wie fange ich mit der Domainregistrierung in Lightsail an?

Nachdem Sie sich bei Lightsail angemeldet haben, können Sie die Lightsail-Konsole verwenden, um Domains zu erstellen und zu verwalten. Weitere Informationen finden Sie unter Domainregistrierung.

Wann sollte ich eine Domain in Lightsail im Vergleich zu Route 53 registrieren?

Aufgaben wie das Registrieren einer Domain, das Erstellen von DNS-Zonen und das Weiterleiten des Datenverkehrs für eine Domain an Lightsail-Ressourcen werden in Lightsail erledigt. Wir empfehlen die Verwendung von Route 53 für fortgeschrittene Aufgaben, z. B. die Verlängerung von Domainregistrierungen, die Übertragung von Domains, einschließlich Datenverkehrsrichtlinien, und die Erstellung privater gehosteter Zonen.

Kann ich meine Domain zu Lightsail übertragen?

Sie können Ihre Domain an Route 53 übertragen. Nach Abschluss der Domainübertragung ist Ihre Domain in der Lightsail-Konsole verfügbar. Weitere Informationen finden Sie unter Verwaltung einer Lightsail-Domain in Amazon Route 53

Welche Lightsail-Ressourcen kann ich mit Domänen verwenden?

Nachdem Sie eine Domain in Lightsail registriert haben, können Sie Ihre Domain auf eine Lightsail-Instance, einen Container, einen Load Balancer, eine statische IP oder ein Content Distribution Network (CDN) verweisen.

Fakturierungs- und Kontenverwaltung

Was kosten Lightsail-Pläne?

Lightsail-Tarife werden nach einem On-Demand-Stundensatz abgerechnet, sodass Sie nur für das bezahlen, was Sie tatsächlich nutzen. Für jeden Lightsail-Tarif, den Sie verwenden, berechnen wir Ihnen den festen Stundenpreis bis zu den maximalen monatlichen Plankosten. Der günstigste Lightsail-Plan beginnt bei 0,0047 USD/Stunde (3,50 USD/Monat). Lightsail-Pläne, die eine Windows Server-Lizenz beinhalten, beginnen bei 0,01075 USD/Stunde (8 USD/Monat).

Wann wird mir ein Plan in Rechnung gestellt?

Lightsail Lightsail-Instanzen und verwaltete Datenbanken fallen Gebühren an, bis sie gelöscht werden. Wenn Sie Ihre Lightsail-Instanz oder verwaltete Datenbank vor Ende des Monats löschen, berechnen wir Ihnen nur anteilige Kosten, basierend auf der Gesamtzahl der Stunden, die Sie Ihre Lightsail-Instanz oder verwaltete Datenbank in diesem Monat genutzt haben. Wenn Sie beispielsweise den günstigsten Lightsail-Instanzplan für 100 Stunden pro Monat verwenden, werden Ihnen 46 Cent (100*0,0046) berechnet.

Kann ich Lightsail-Instances kostenlos testen?

Ja! Egal, ob Sie bereits AWS Kunde oder Neukunde sind, Sie erhalten 750 Stunden kostenlose Nutzung des Lightsail-Plans im Wert von 3,50 USD. Sie können Lightsail-Pläne, die eine Windows Server-Lizenz enthalten, auch kostenlos testen, wenn Sie den Windows-Plan für 8 USD verwenden.

Sie können mit Ihre 750 Stunden auf beliebig viele Instances aufteilen. Sie können beispielsweise eine einzelne Lightsail-Instance für einen ganzen Monat oder 10 Lightsail-Instances für 75 Stunden ausführen. Das kostenlose Testangebot gilt nur für die Nutzung innerhalb des ersten Kalendermonats ab Ihrer Registrierung für Lightsail. Wenn Ihr Konto mit einer Organisation (unter AWS Organizations) verknüpft ist, kann nur ein Konto innerhalb der Organisation von den Angeboten für das kostenlose Kontingent von AWS profitieren.

> **Note**
>
> Im Rahmen des AWS kostenlosen Kontingents können Sie Amazon Lightsail für ausgewählte Instance-Pakete kostenlos nutzen. Weitere Informationen finden Sie unter AWS Kostenloses Kontingent auf der Preisseite von Amazon Lightsail.

Wann beginnt die kostenlose Lightsail-Testversion?

Die Vorteile der kostenlosen Lightsail-Testversion beginnen, wenn die erste Ressource, die für die kostenlose Testversion in Frage kommt, veröffentlicht wird.

Die erweiterte kostenlose 90-Tage-Testversion für Instances und Datenbanken gilt nur für ausgewählte Pläne (Bundles). Das Angebot gilt für neue oder bestehende AWS Konten, die Lightsail am oder nach dem 8. Juli 2021 nutzen. Weitere Informationen finden Sie in der Lightsail-Preisliste.

Was kosten verwaltete Lightsail-Datenbanken?

Von Lightsail verwaltete Datenbanken sind in 4 Plangrößen erhältlich und beginnen bei 15 USD pro Monat für eine 1-GB-RAM-Datenbankinstanz mit 40 GB SSD-Speicher und 100 GB Datenübertragungskapazität. Hochverfügbarkeitspläne kosten das Doppelte der Standardpläne, da sie eine zusätzliche Datenbank-Instance und Speicherplatte in einer anderen Availability Zone zur Redundanz enthalten.

Kann ich verwaltete Lightsail-Datenbanken kostenlos testen?

Ja! Neue Lightsail-Kunden erhalten 1 Monat des Lightsail-Plans im Wert von 15 USD kostenlos.

Was kostet Lightsail-Blockspeicher?

Lightsail-Blockspeicher kostet 0,10 USD pro GB und Monat.

Was kosten Lightsail Load Balancer?

Lightsail Load Balancer kosten 18 USD pro Monat.

Wie viel kostet die Zertifikatsverwaltung?

Lightsail-Zertifikate und Zertifikatsverwaltung sind bei Verwendung eines Lightsail-Loadbalancers kostenlos.

Was kosten statische Lightsail-IPv4-Adressen?

Statische IP-Adressen sind mit keinen Kosten verbunden, wenn sie an eine Lightsail-Instance angehängt werden. Statische IPs können nicht an reine IPv6-Instances angehängt werden. IPv4-Adressen sind eine knappe Ressource und Lightsail engagiert sich dafür, sie effizient zu nutzen. Deshalb berechnen wir eine geringe Gebühr von 0,005 USD/Stunde für statische IPs, die länger als 1 Stunde nicht an eine Instance angehängt sind.

Was kostet die Datenübertragung?

Ihre Pläne für Instance, Datenbank und Content-Delivery-Network (CDN)-Verteilungen enthalten eine Datenübertragungszulage.

Bei Lightsail-Instances werden sowohl eingehende als auch ausgehende Datenübertragungen auf Ihre Datenübertragungsmenge angerechnet. Wenn Sie Ihr Datenübertragungslimit überschreiten, wird Ihnen nur die ausgehende Datenübertragung von einer Lightsail-Instance ins Internet oder zu AWS Ressourcen, die die öffentliche IP-Adresse der Instance verwenden, in Rechnung gestellt. Sowohl die eingehende Datenübertragung zu Lightsail-Instances als auch die ausgehende Datenübertragung von einer Lightsail-Instance, wenn Sie die private IP-Adresse der Instance verwenden, sind über Ihre Datenübertragungsrechte hinaus kostenlos.

Bei von Lightsail verwalteten Datenbanken wird nur die ausgehende Datenübertragung auf Ihre Zulage angerechnet. Wenn Sie Ihr Datenübertragungslimit überschreiten, wird Ihnen nur die ausgehende Datenübertragung von einer von Lightsail verwalteten Datenbank ins Internet in Rechnung gestellt.

Bei Lightsail-CDN-Distributionen werden alle Datenübertragungen aus Ihrer Distribution auf Ihr Kontingent angerechnet. Für jede Datenübertragung, die AUS Ihrer Verteilung übertragen wird, wird Ihnen eine Gebühr in Rechnung gestellt, nachdem die zulässige Datenübertragung Ihrer Verteilung überschritten ist.

Wie wirkt sich die Verwendung der Load Balancer auf mein Kontingent für die Datenübertragung aus?

Ihr Load Balancer wirkt sich nicht auf Ihr Kontingent für die Datenübertragung aus. Der Datenverkehr zwischen dem Load Balancer und den Ziel-Instances oder -Distributionen wird gemessen und auf Ihre Datenübertragungsmenge für Ihre Instances oder Distributionen angerechnet, genauso wie der ein- und ausgehende Datenverkehr zum Internet auf Ihre Datenübertragungsmenge für Lightsail-Instances angerechnet wird, die sich nicht hinter einem Load Balancer befinden. Datenverkehr in und aus Ihrem Load Balancer zum Internet wird dem Kontingent für die Datenübertragung Ihrer Instance nicht abgezogen.

Was passiert, wenn ich mein Datenübertragungsplan-Kontingent überschreite?

Wir haben unsere Datenübertragungspläne so ausgelegt, dass die Mehrzahl unserer Kunden von ihrem Kontingent abgedeckt werden und ihnen keine zusätzlichen Gebühren anfallen. Wenn Ihre Instance das Datenübertragungsplan-Kontingent überschreitet, wird Ihnen eine Überschreitungsgebühr pro GB genutzte Datenübertragung berechnet (nur AUS Datenübertragung ins Internet).

Selbst wenn Ihre Instance das Datenübertragungsplan-Kontingent überschreitet, sind noch viele Arten von Datenübertragungen kostenlos. Die eingehende Datenübertragung zu Lightsail-Instanzen und Datenbanken ist immer kostenlos. Die ausgehende Datenübertragung von einer Lightsail-Instanz zu einer anderen Lightsail-Instanz, zwischen Lightsail-Instanzen und von Lightsail verwalteten Datenbanken oder zu AWS Ressourcen in derselben Region ist ebenfalls kostenlos, wenn private IP-Adressen verwendet werden.

Welche Arten von Datenübertragungen werden mir in Rechnung gestellt?

Wenn Sie die monatliche kostenlose Datenübertragungsmenge Ihres Instance-Plans überschreiten, wird Ihnen die ausgehende Datenübertragung von einer Lightsail-Instance ins Internet oder zu einer anderen AWS-Region oder zu AWS Ressourcen in derselben Region in Rechnung gestellt, wenn Sie öffentliche IP-Adressen verwenden. Die Gebühr für diese Art von Datenübertragung über das kostenlose Kontingent hinaus beträgt:

- USA Ost (Ohio) (us-east-2): 0,09 USD/GB
- USA Ost (Nord-Virginia): (us-east-1): 0,09 USD/GB
- USA West (Oregon): (us-west-2): 0,09 USD/GB
- Asien-Pazifik (Mumbai): (ap-south-1): 0,13 USD/GB
- Asien-Pazifik (Seoul): (ap-northeast-2): 0,13 USD/GB
- Asien-Pazifik (Singapur): (ap-southeast-1): 0,12 USD/GB
- Asien-Pazifik (Sydney): (ap-southeast-2): 0,17 USD/GB
- Asien-Pazifik (Tokio): (ap-northeast-1): 0,14 USD/GB
- Kanada (Zentral): (ca-central-1): 0,09 USD/GB
- EU (Frankfurt): (eu-central-1): 0,09 USD/GB
- EU (Irland): (eu-west-1): 0,09 USD/GB
- EU (London): (eu-west-2): 0,09 USD/GB
- EU (Paris): (eu-west-3): 0,09 USD/GB
- Europa (Stockholm) (eu-north-1): 0,09 USD/GB

Instances, die in unterschiedlichen Availability Zones erstellt werden, können privat und kostenlos zwischen Zonen kommunizieren, und es ist sehr viel unwahrscheinlicher, dass sie gleichzeitig

beeinträchtigt werden. Availability Zones ermöglichen Ihnen, hoch verfügbare Anwendungen und Websites zu entwickeln, ohne dabei die Kosten der Datenübertragung zu erhöhen oder die Sicherheit Ihrer Anwendung zu beeinträchtigen.

Wenn Sie die Datenübertragungsmenge Ihres Lightsail CDN-Vertriebsplans überschreiten, werden Ihnen alle ausgehenden Datenübertragungen in Rechnung gestellt. Die Gebühren für Datenübertragungen, die das für Ihren Vertrieb festgelegte Kontingent überschreiten, unterscheiden sich von denen für Lightsail-Instances und lauten wie folgt:

- Asien-Pazifik: 0,13 USD/GB
- Kanada: 0,09 USD/GB
- Europa: 0,09 USD/GB
- Indien: 0,13 USD/GB
- Japan: 0,14 USD/GB
- Mittlerer Osten: 0,11 USD/GB
- Südafrika: 0,11 USD/GB
- Südamerika: 0,11 USD/GB
- Vereinigte Staaten: 0,09 USD/GB

Wie variieren die Berechtigungen für meinen Instance-Datenübertragungsplan nach AWS-Region?

Mit Ausnahme der Regionen Asien-Pazifik (Mumbai) und Asien-Pazifik (Sydney) gilt für alle AWS-Region Geräte das gleiche Datenübertragungsvolumen wie auf amazonlightsail.com und amazonlightsail.com/pricing aufgeführt. In diesen beiden Fällen AWS-Region ist das zulässige Datenübertragungspaket für Instances wie folgt:

- 3,50 USD/Monat-Plan: 0,5 TB
- 5 USD/Monat-Plan: 1 TB
- 10 USD/Monat-Plan: 1,5 TB
- 20 USD/Monat-Plan: 2 TB
- 40 USD/Monat-Plan: 2,5 TB

- 80 USD/Monat-Plan: 3 TB
- 160 USD/Monat-Plan: 3,5 TB

Die Datenübertragungsberechtigungen für von Lightsail verwaltete Datenbanken sind in allen Regionen gleich.

Wie funktioniert mein Datenübertragungskontingent für Instances?

Jeder Lightsail-Instanzplan beinhaltet eine Datenübertragungszulage. Mit dem Tarif von 3,50 USD pro Monat kann Ihre Instance monatlich beispielsweise bis zu 1 TB Daten in das Internet senden und aus dem Internet erhalten, ohne zusätzliche Kosten. Ihr Datenübertragungskontingent wird jeden Monat zurückgesetzt, und Ihre Instance kann es bei Bedarf innerhalb des Monats nutzen.

Nachdem Ihre Instance das Datenübertragungskontingent für den Monat erreicht hat, wird die Datenübertragung ins Internet ab 0,09 USD pro GB in Rechnung gestellt, abhängig von der AWS-Region , in der sich Ihre Instance befindet. Wenn Sie Ihre Instance löschen und im selben Monat eine weitere erstellen, wird das kostenlose Datenübertragungsvolumen zwischen den beiden Instances aufgeteilt. AWS-Region

Was kosten Lightsail-Domains?

Die in der verknüpften PDF-Datei aufgeführten Preise gelten für neue Domänennamenregistrierungen und Verlängerungen bestehender Domänennamenregistrierungen ab dem 22. Dezember 2021. Alle Preise beinhalten eine DNS-Zone und Datenschutz. Informationen zu den Kosten für die Registrierung von Domains finden Sie unter Preise von Amazon Route 53 für die Domainregistrierung und Domainregistrierung.

Was kostet Lightsail DNS-Management?

Die DNS-Verwaltung ist in Lightsail kostenlos. Sie können bis zu 6 DNS-Zonen und beliebig viele Datensätze für jede DNS-Zone erstellen. Sie erhalten außerdem ein monatliches Kontingent von 3 Millionen DNS-Abfragen pro Monat für Ihre Zonen. Über die ersten drei Millionen Abfragen in einem Monat hinaus werden Ihnen pro Million DNS-Abfragen 0,40 USD in Rechnung gestellt.

Was kosten Lightsail-Snapshots?

Die Speicherung von Lightsail-Snapshots (manuell und automatisch) kostet 0,05 USD/GB pro Monat. Das bedeutet, dass Sie, wenn Sie einen Snapshot einer Instance erstellen, die 28 GB Speicherplatz nutzt und diesen für einen Monat behalten, 1,40 USD für den Monat bezahlen.

Wenn Sie mehrere aufeinanderfolgende Snapshots derselben Instanz erstellen, optimiert Lightsail Ihre Snapshots automatisch kostenoptimiert. Bei jedem neuen Snapshot, den Sie erstellen, wird

nur der Teil der Daten in Rechnung gestellt, der sich geändert hat. Wenn sich im obigen Beispiel Ihre Daten nur um 2 GB ändert, kostet Ihr zweiter Instance-Snapshot nur 0,10 USD pro Monat.

Wie kann ich mein AWS -Konto verwalten?

Lightsail ist ein AWS Dienst und läuft auf der AWS vertrauenswürdigen und bewährten Cloud-Infrastruktur. Sie verwenden dasselbe AWS Konto und dieselben Anmeldeinformationen, um sich bei Lightsail und der AWS-Managementkonsole anzumelden.

Sie können Ihr AWS Konto über die Billing and Cost Management-Konsole verwalten, einschließlich der Änderung Ihres AWS Kontokennworts, Ihres Benutzernamens, Ihrer Kontaktinformationen oder Ihrer AWS Rechnungsinformationen.

Was sind die rechtlichen Nutzungsbedingungen von Lightsail?

Lightsail ist ein Amazon-Webservice. Um Lightsail nutzen zu können, stimmen Sie zunächst der AWS Kundenvereinbarung und den Servicebedingungen zu. Bei der Erstellung von Lightsail-Instanzen erklären Sie sich außerdem damit einverstanden, dass Ihre Nutzung der Software auch der Endbenutzer-Lizenzvereinbarung des Verkäufers unterliegt, die Sie auf der Seite „Instanz erstellen“ einsehen können.

Wie kann ich meine Lightsail-Rechnung bezahlen?

Sie können Ihre Rechnung über die AWS Billing and Cost Management-Konsole bezahlen und verwalten. AWS akzeptiert die meisten gängigen Kreditkarten. Hier erfahren Sie mehr über die Verwaltung Ihrer Zahlungsmethoden.

In Amazon Elastic Compute Cloud (Amazon EC2) exportieren

Was ist Export nach Amazon EC2?

Der Export nach Amazon EC2 ist eine Funktion, mit der Sie eine Kopie Ihrer Lightsail-Instance in Amazon EC2 erstellen können. Wenn Sie nach Amazon EC2 exportieren, können Sie aus der Vielzahl der Instance-Typen, Konfigurationen und Preismodelle auswählen, die Amazon EC2 bietet. Sie haben dann eine noch präzisere Kontrolle über Ihre Netzwerk-, Speicher- und Datenverarbeitungsumgebung.

Warum sollte ich nach Amazon EC2 exportieren wollen?

Lightsail bietet Ihnen eine einfache Möglichkeit, eine Vielzahl von Cloud-basierten Anwendungen zu einem gebündelten, vorhersehbaren und niedrigen Preis auszuführen und zu skalieren.

Lightsail richtet auch automatisch Ihre Cloud-Umgebungskonfigurationen wie Netzwerk- und Zugriffsmanagement ein.

Der Export nach Amazon EC2 ermöglicht es Ihnen, Ihre Anwendung auf einer größeren Anzahl von Instance-Typen auszuführen, die von virtuellen Maschinen mit mehr CPU-Leistung, Arbeitsspeicher und Netzwerkfähigkeiten bis hin zu speziellen oder schnelleren Instances mit FPGAs und GPUs reichen. Darüber hinaus führt Amazon EC2 weniger automatische Verwaltung und Einrichtung durch, sodass Sie mehr Kontrolle darüber haben, wie Sie Ihre Cloud-Umgebung (z. B. Ihre VPC) konfigurieren.

Wie funktioniert der Export nach Amazon EC2?

Um zu beginnen, müssen Sie Ihren manuellen Snapshot einer Lightsail-Instanz oder eines Blockspeicherdatenträgers exportieren. Kunden, die mit Amazon EC2 vertraut sind, können dann mit dem Amazon-EC2-Erstellungsassistenten oder der API eine neue Amazon-EC2-Instance oder ein Amazon-EBS-Volume erstellen, wie sie es von einem bestehenden EC2-, AMI- oder EBS-Volumen gewohnt sind. Alternativ bietet Lightsail auch eine geführte Lightsail-Konsolenoberfläche, mit der Sie auf einfache Weise eine neue EC2-Instance erstellen können.

> **Note**
>
> Snapshots von cPanel und WHM, Django und Ghost-Instances können derzeit nicht nach Amazon EC2 exportiert werden.

Wie wird dies für mich in Rechnung gestellt?

Die Verwendung des Export-Features nach Amazon EC2 ist kostenlos. Sobald Sie Ihre manuellen Snapshots nach Amazon EC2 exportiert haben, wird Ihnen das Amazon EC2 EC2-Image separat und zusätzlich zu Ihrem manuellen Lightsail-Snapshot in Rechnung gestellt. Alle neuen Amazon-EC2-Instances, die Sie starten, werden ebenfalls von Amazon EC2 berechnet – einschließlich ihrer Amazon-EBS-Speichervolumen und des Datentransfers. Einzelheiten zu den Preisen für Ihre neue Instance und Ressourcen finden Sie auf der Amazon-EC2-Preisseite. Lightsail-Ressourcen, die weiterhin in Ihrem Lightsail-Konto laufen, werden weiterhin zu ihren regulären Tarifen abgerechnet, bis sie gelöscht werden.

Kann ich verwaltete Datenbanken oder Datenträger-Snapshots exportieren?

Die Exportfunktion ermöglicht es Ihnen, manuelle Lightsail-Festplatten-Snapshots zu exportieren, unterstützt derzeit jedoch keine manuellen Snapshots von verwalteten Datenbanken. Datenträger-

Snapshots können über die Konsole oder die API von Amazon EC2 als Amazon-EBS-Volumen wiederverwendet werden.

Welche Lightsail-Ressourcen kann ich exportieren?

Die Funktion Lightsail-Export nach Amazon EC2 wurde entwickelt, um den Export von Linux- und Windows-Instance-Snapshots nach Amazon EC2 zu unterstützen. Es unterstützt auch den Export von Snapshots von Blockspeicherdatenträgern nach Amazon EBS. Sie unterstützt derzeit nicht den Export von Datenbanken, Container-Services, Content-Delivery-Network (CDN)-Verteilungen, Load Balancer, statischen IPs und DNS-Datensätzen. Außerdem können Snapshots von Django, Ghost und cPanel und WHM-Instances derzeit nicht nach Amazon EC2 exportiert werden.

Schlagworte in Lightsail

Was sind Tags?

Ein Tag ist eine Bezeichnung, die Sie einer Lightsail-Ressource zuweisen. Jedes Tag besteht aus einem Schlüssel und einem Wert, die Sie beide selbst definieren können. Ein Tagwert ist optional, Sie können also festlegen, dass nur Schlüssel verwendet werden, um Ressourcen in der Lightsail-Konsole zu filtern.

Wie kann ich Tags in Lightsail verwenden?

Tags haben mehrere Anwendungsfälle: Sie ermöglichen es Ihnen, Ihre Ressourcen in der Lightsail-Konsole und API zu gruppieren und zu filtern, Ihre Kosten in Ihrer Rechnung zu verfolgen und zu organisieren und mithilfe von Zugriffsverwaltungsregeln zu regeln, wer Ihre Ressourcen sehen oder ändern kann. Das Markieren von Ressourcen bietet Ihnen folgenden Möglichkeiten:

• Organisieren — Verwenden Sie die Lightsail-Konsole und API-Filter, um Ressourcen anhand ihrer Tags, die Sie ihnen zugewiesen haben, anzuzeigen und zu verwalten. Dies ist hilfreich, wenn Sie viele Ressourcen desselben Typs haben. In diesem Fall können Sie basierend auf den zugewiesenen Tags schnell bestimmte Ressourcen identifizieren.

• Kostenzuordnung: Verfolgen und verteilen Sie Kosten auf verschiedene Projekte oder Benutzer, indem Sie Ihre Ressourcen markieren und "Kostenzuordnungs-Tags" in der Abrechnungskonsole erstellen. So können Sie beispielsweise Ihre Rechnung aufteilen und Ihre Kosten projekt- oder kundenbezogen nachvollziehen.

• Zugriff verwalten — Steuern Sie mithilfe AWS Identity and Access Management von Richtlinien, wie Benutzer mit Zugriff auf Ihr AWS Konto Lightsail-Ressourcen bearbeiten, erstellen und

löschen können. Auf diese Weise können Sie einfacher mit anderen zusammenarbeiten, ohne ihnen vollen Zugriff auf Ihre Lightsail-Ressourcen gewähren zu müssen.

Weitere Informationen zur Verwendung von Tags in Lightsail finden Sie unter Tags.

Welche Ressourcen können getaggt werden? >

Lightsail unterstützt derzeit Tagging für die folgenden Ressourcen:

- Instances (Linux und Windows)
- Container-Services
- Blockspeicherdatenträger
- Load Balancer
- Datenbanken
- DNS-Zonen
- Manuelle Snapshots von Instances, Datenträgern und Datenbanken

Manuelle Schnappschüsse unterstützen Tags. Sie müssen jedoch die Lightsail-API oder das Taggen von AWS CLI Schnappschüssen verwenden. Wenn Sie die Lightsail-Konsole verwenden, um einen manuellen Snapshot einer markierten Instanz, Festplatte oder Datenbank zu erstellen, erhält der manuelle Snapshot automatisch dieselben Tags wie die Quellressource. Sie können diese Tags bearbeiten, wenn Sie die Lightsail-Konsole verwenden, um eine neue Ressource aus einem mit Tags versehenen manuellen Snapshot zu erstellen.

Automatische Snapshots können nicht markiert werden.

Wie kann ich meine Lightsail-Schnappschüsse taggen?

Die Lightsail-Konsole kennzeichnet manuelle Snapshots automatisch mit denselben Tags wie ihre Quellressource. Wenn Sie die Lightsail-API verwenden oder einen Snapshot erstellen AWS CLI möchten, können Sie die Tags für den Snapshot selbst auswählen.

> **Important**
>
> Tags für manuelle Snapshots von Datenbanken sind derzeit nicht in Fakturierungsberichten enthalten (Kostenzuordnungs-Tags).

Was ist der Unterschied zwischen Key-Value- und Key-only-Tags?

Lightsail-Tags sind Schlüssel-Wert-Paare, mit denen Sie Ressourcen wie Instanzen in verschiedenen Kategorien organisieren können (z. B. project:Blog, project:Game, project:Test). Dies ermöglicht Ihnen die volle Kontrolle über alle Anwendungsfälle wie Ressourcenorganisation, Rechnungsberichte und Zugriffsverwaltung. Die Lightsail-Konsole ermöglicht es Ihnen auch, Ihre Ressourcen mit Tags zu kennzeichnen, die nur auf Tastenkürzel beschränkt sind, um in der Konsole schnell zu filtern.

Kontakte und Benachrichtigungen

Was sind Benachrichtigungen?

Sie können Alarme in Lightsail konfigurieren, damit Sie benachrichtigt werden, wenn eine Metrik für eine Ihrer Instanzen, Datenbanken oder Load Balancer einen bestimmten Schwellenwert überschreitet. Benachrichtigungen können die Form eines Banners aufweisen, das in der Lightsail-Konsole angezeigt wird, einer E-Mail, die an eine von Ihnen angegebene Adresse gesendet wird, oder einer SMS, die an eine von Ihnen angegebene Mobiltelefonnummer gesendet wird. Um per E-Mail und SMS-Textnachricht benachrichtigt zu werden, müssen Sie in jedem Bereich, in AWS-Region dem Sie Ihre Ressourcen überwachen möchten, Ihre E-Mail-Adresse und Handynummer als Benachrichtigungskontakte hinzufügen. Weitere Informationen zu Benachrichtigungen finden Sie unter Benachrichtigungen.

Wie viele Kontakte kann ich hinzufügen?

Sie können jeweils eine E-Mail-Adresse und eine Handynummer hinzufügen, unter AWS-Region der Sie Ihre Ressourcen überwachen möchten. SMS-Textnachrichten werden nicht in allen AWS-Region s unterstützt, in denen Sie Lightsail-Ressourcen erstellen können, und Textnachrichten können nicht in einige Länder und Regionen der Welt gesendet werden. Weitere Informationen zu Benachrichtigungen finden Sie unter Benachrichtigungen.

Metriken und Alarme

Was sind Metriken?

Lightsail meldet Metrikdaten für Instances, Datenbanken und Load Balancer. Einige Metriken enthalten die CPU-Auslastung Ihrer Instance in Prozent, die Menge des eingehenden und ausgehenden Netzwerkverkehrs, System- und Instance-Fehleranzahl, die Tiefe der Datenbank-

Datenträgerwarteschlange, den freien Speicherplatz in der Datenbank, die Fehleranzahl des Load Balancers, Reaktionszeiten der Load Balancer und vieles mehr. Metriken ermöglichen das Überwachen und Aufrechterhalten der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer Ressourcen. Überwachen und sammeln Sie regelmäßig Metrikdaten von Ihren Ressourcen, damit Sie bei Auftreten eines Mehrpunkt-Fehlers diesen leichter debuggen können. Weitere Informationen finden Sie unter Ressourcenmetriken.

Was sind Alarme?

Sie können in Lightsail einen Alarm erstellen, der eine Metrik für Ihre Instances, Datenbanken und Load Balancer überwacht. Der Alarm kann so konfiguriert werden, dass Sie basierend auf dem Wert der Metrik relativ zu einem von Ihnen angegebenen Schwellenwert benachrichtigt werden. Weitere Informationen finden Sie unter -Alarme.

Benachrichtigungen können ein in der Lightsail-Konsole angezeigtes Banner, eine an Ihre E-Mail-Adresse gesendete E-Mail oder eine an Ihre Mobiltelefonnummer gesendete SMS-Nachricht sein. Weitere Informationen zu Benachrichtigungen finden Sie unter Benachrichtigungen.

Wie viele Alarme kann ich hinzufügen?

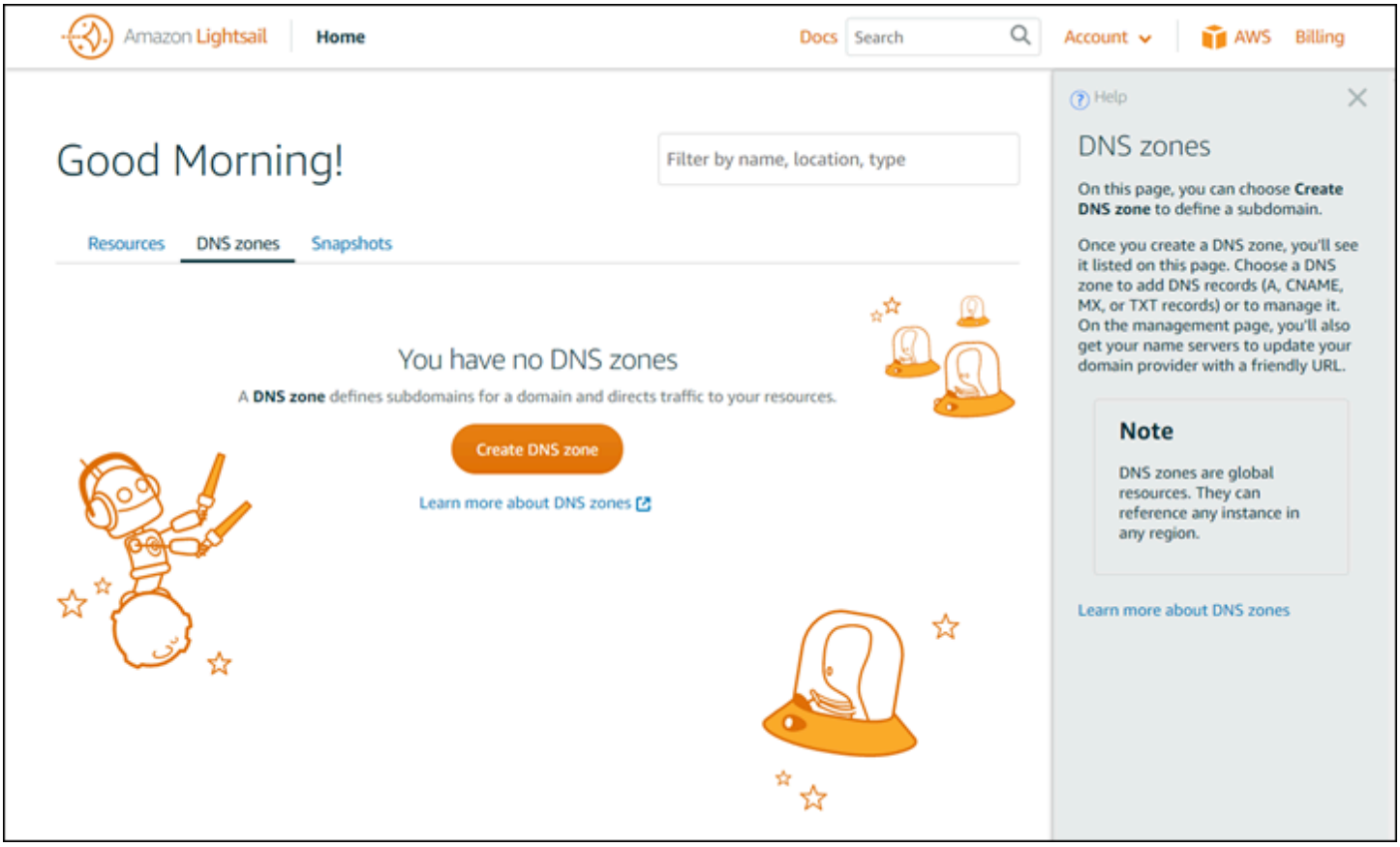
Sie können zwei Alarme für jede Metrik konfigurieren, die für Instances, Datenbanken und Load Balancer verfügbar ist. Weitere Informationen finden Sie unter -Alarme.

Erhalten Sie Hilfe mit Amazon Lightsail

Es gibt mehrere Möglichkeiten, wie Sie in Amazon Lightsail Hilfe erhalten können.

Kontextsensitives Hilfefeld

Lightsail verfügt auf jeder Seite der Konsole über eine kontextbezogene Help (Hilfe) mit zusätzlichen Tipps und Informationen, die sich auf die Seite beziehen, auf der Sie sich gerade befinden. Öffnen Sie die Hilfe, wenn Sie eine Frage zu einem Thema auf der Seite haben, und schließen Sie, wenn Sie bereit für die Erledigung der Aufgabe sind. Sie öffnen die Hilfe, indem Sie auf einer Seite Help (Hilfe) auswählen, oder indem Sie auf eines der kleinen Fragezeichen auf der Benutzeroberfläche klicken.



Über dieses Benutzerhandbuch

Das Amazon Lightsail-Entwicklerhandbuch enthält Themen mit schrittweisen Anleitungen und konzeptionelle Übersichten, die Ihnen bei der Arbeit in Lightsail helfen. Beispielsweise können Sie eine Instance erstellen, eine Verbindung zu Ihrer Instance herstellen oder Ihre Domäne verwalten.

Verwenden der Suche

Über das Suchfeld oben auf jeder Seite können Sie von jeder Seite in Lightsail aus nach Dokumentationsthemen suchen. Zur Verfeinerung Ihrer Suche können Sie jederzeit von der Dokumentationssuche aus suchen.

Sie finden nicht, was Sie suchen? Das tut uns leid! Senden Sie uns Ihr Feedback, wir werden uns darum kümmern. Sie können auf jeder Seite in Lightsail Questions? auswählen. Comments? (Fragen? Kommentare?) wählen und Feedback übermitteln, um Vorschläge zu machen. Wir werden Ihnen antworten.

Verwenden der Lightsail-CLI und des API

Sie können die AWS Command Line Interface (AWS CLI) oder das Lightsail-REST-API verwenden, um Lightsail-Ressourcen zu erstellen, zu lesen, zu aktualisieren und zu löschen. Zusätzlich zu dem REST-API verfügen wir über ein SDK in mehreren Sprachen, darunter Java, Ruby, JavaScript (Node.js), Go, PHP, Python,.NET (C #) und C++. Weitere Informationen zur Lightsail-API finden Sie in der Lightsail-API-Referenz.

> **Note**
>
> Sie müssen Zugriffsschlüssel generieren, um das Lightsail-API nutzen zu können. Weitere Informationen zum Einrichten von Zugriffsschlüsseln für die Nutzung der Lightsail-API.

Die AWS CLI ist hilfreich, wenn Sie mit Lightsail-Ressourcen arbeiten. Geben Sie in die AWS-AWS CLI einfach `aws lightsail help` ein, um mehr über die verfügbaren Befehle zu erfahren. Wenn Sie Hilfe zu einem bestimmten CLI-Befehl benötigen, geben Sie den Befehl `help` ein, gefolgt von Parametern und Ausnahmen, um weitere Informationen zu den Namen zu erhalten. Weitere Informationen finden Sie in der Lightsail-CLI-Referenz.

AWS-Foren und andere Community-Ressourcen

Sie können Ihre Fragen auch in unserem AWS-Diskussionsforum veröffentlichen: AWS-Foren.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.