Handbuch „Erste Schritte“

AWS Management Console

Version 1.0

AWS Management Console: Handbuch „Erste Schritte“

Table of Contents

Was ist der AWS Management Console?

Dabei AWS Management Consolehandelt es sich um eine Webanwendung, die eine breite Sammlung von Servicekonsolen für die Verwaltung AWS von Ressourcen umfasst und sich auf diese bezieht. Wenn Sie sich zum ersten Mal anmelden, sehen Sie die Startseite der Konsole. Die Startseite bietet Zugriff auf jede Servicekonsole und bietet einen einzigen Ort, an dem Sie auf die Informationen zugreifen können, die Sie zum Ausführen Ihrer AWS zugehörigen Aufgaben benötigen. Außerdem können Sie die Console-Home-Oberfläche anpassen, indem Sie Widgets wie „Zuletzt besucht“, „AWS Health“ und mehr hinzufügen, entfernen und neu anordnen.

> **Note**
>
> Die Sprachauswahloption wurde auf die neue Seite „Unified Settings“ (Einheitliche Einstellungen) verschoben. Weitere Informationen finden Sie unter Ändern der Sprache der AWS Management Console.

Die einzelnen Servicekonsolen bieten dagegen ein breites Spektrum an Tools für Cloud Computing sowie Informationen über Ihr Konto und über Ihre Fakturierung.

Verwenden des gewünschten Geräts

Die AWS Management Console kann sowohl auf Tablets als auch auf anderen Geräten eingesetzt werden:

- Der horizontale und vertikale Anzeigeplatz wurden maximiert, damit mehr Inhalte auf dem Bildschirm angezeigt werden können.

- Für eine optimierte Touch-Umgebung wurden Schaltflächen und Auswahlen vergrößert.

Das AWS Management Console ist auch als App für Android und iOS verfügbar. Diese App unterstützt für den Mobilbetrieb geeignete Aufgaben und ergänzt die umfassende Browsererfahrung. Sie können beispielsweise Ihre vorhandenen Amazon EC2-Instances und CloudWatch Amazon-Alarme ganz einfach von Ihrem Telefon aus anzeigen und verwalten.

Sie können die mobile AWS Konsolen-App aus dem Amazon Appstore, Google Play oder iTunes herunterladen.

Konfiguration der AWS Management Console

In diesem Thema wird beschrieben, wie Sie Ihre Einstellungen konfigurieren AWS Management Console und wie Sie die Seite mit den vereinheitlichten Einstellungen verwenden, um Standardwerte festzulegen, die für alle Servicekonsolen gelten. Außerdem werden Widgets erklärt, eine Funktion des Dashboards auf der Startseite der Konsole, mit der Sie benutzerdefinierte Komponenten hinzufügen können, mit denen Sie Informationen über Ihre AWS Dienste und Ressourcen verfolgen können.

Themen

Arbeiten mit Widgets

Das Console Home-Dashboard enthält Widgets, die wichtige Informationen über Ihre AWS Umgebung anzeigen und Verknüpfungen zu Ihren Diensten bereitstellen. Sie können Ihre Umgebung anpassen, indem Sie Widgets hinzufügen und entfernen, sie neu anordnen oder ihre Größe ändern.

So fügen Sie ein Widget hinzu:

1. Wählen Sie oben oder unten rechts auf dem Dashboard auf der Konsolenstartseite die Schaltfläche Widgets hinzufügen aus.
2. Wählen Sie den Schleppzeiger aus, der durch sechs vertikale Punkte oben links in der Widget-Titelleiste dargestellt wird, und ziehen Sie ihn auf Ihr Dashboard auf der Konsolenstartseite.

So entfernen Sie ein Widget

1. Wählen Sie die Ellipse aus, die durch drei vertikal angeordnete Punkte oben rechts in der Titelleiste des Widgets angezeigt wird.

2. Wählen Sie Remove widget (Widget entfernen) aus.

So ordnen Sie Ihre Widgets neu an

- Wählen Sie den Schleppzeiger aus, der durch sechs vertikale Punkte oben links in der Widget-Titelleiste dargestellt wird, und ziehen Sie das Widget an die gewünschte Stelle im Dashboard auf der Konsolenstartseite.

So ändern Sie die Größe eines Widgets

- Wählen Sie das Symbol zur Größenänderung oben rechts im Widget aus und passen Sie die Größe des Widgets an.

Wenn Sie mit dem Organisieren und Einrichten Ihrer Widgets von vorne beginnen möchten, können Sie das Dashboard auf der Konsolenstartseite auf das Standardlayout zurücksetzen. Hierdurch werden Ihre Änderungen am Layout des Dashboards auf der Konsolenstartseite zurückgesetzt und alle Widgets werden zum Standardspeicherort und zur Standardgröße wiederhergestellt.

So setzen Sie die Seite auf das Standardlayout zurück:

1. Wählen Sie oben rechts auf der Seite Reset to default layout (Auf das Standardlayout zurücksetzen) aus.
2. Wählen Sie zur Bestätigung Reset (Zurücksetzen) aus.

> **Note**
>
> Anschließend werden alle Änderungen am Layout der Dashboards auf der Konsolenstartseite zurückgesetzt.

So fordern Sie ein neues Widget im Dashboard auf der Konsolenstartseite an

1. Wählen Sie unten links im Dashboard auf der Konsolenstartseite Want to see another widget? (Möchten Sie ein anderes Widget sehen?) aus. Sagen Sie es uns!

   Beschreiben Sie das Widget, das Sie im Dashboards auf der Konsolenstartseite sehen möchten.
2. Wählen Sie Absenden aus.

> **Note**
>
> Wir überprüfen Ihre Vorschläge regelmäßig und fügen möglicherweise in zukünftigen Updates der AWS Management Console neue Widgets hinzu.

Konfigurieren der einheitlichen Einstellungen

Sie können Einstellungen und Standardeinstellungen wie Anzeige, Sprache und Region auf der Seite „ AWS Management Console Vereinheitlichte Einstellungen“ konfigurieren. Der visuelle Modus und die Standardsprache können auch direkt über die Navigationsleiste eingestellt werden. Diese Änderungen gelten für alle Servicekonsolen.

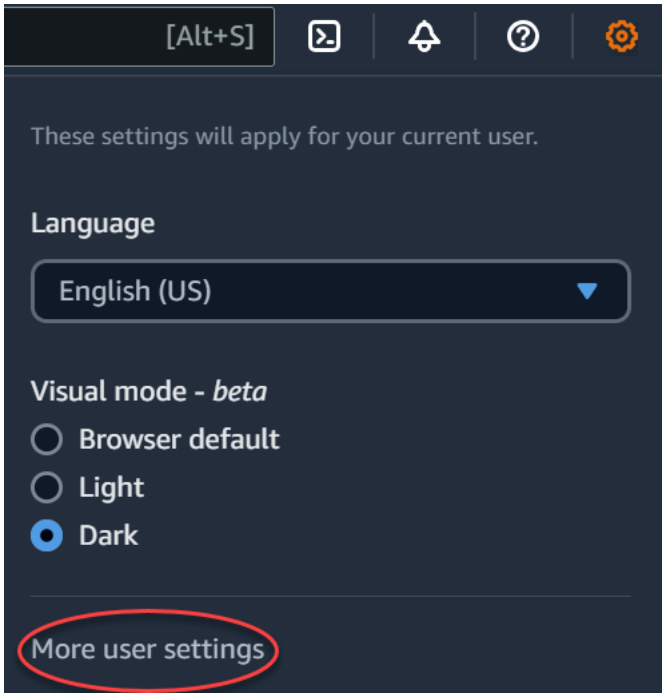
> **Important**
>
> Um sicherzustellen, dass Ihre Einstellungen, bevorzugten Dienste und kürzlich besuchten Dienste weltweit bestehen, werden diese Daten in allen gespeichert AWS-Regionen, auch in Regionen, die standardmäßig deaktiviert sind. Diese Regionen sind Afrika (Kapstadt), Asien-Pazifik (Hongkong), Asien-Pazifik (Hyderabad), Asien-Pazifik (Jakarta), Europa (Mailand), Europa (Spanien), Europa (Zürich), Naher Osten (Bahrain) und Naher Osten (VAE). Sie müssen nach wie vor eine Region manuell aktivieren, um auf sie zugreifen und anschließend Ressourcen in dieser Region verwalten zu können. Wenn Sie diese Daten nicht in allen speichern möchten AWS-Regionen, wählen Sie Alle zurücksetzen, um Ihre Einstellungen zu löschen, und deaktivieren Sie dann in der Einstellungsverwaltung die Speicherung kürzlich besuchter Dienste.

Zugreifen auf vereinheitlichte Einstellungen

Im folgenden Verfahren wird beschrieben, wie Sie auf Unified Settings zugreifen.

So greifen Sie auf die einheitlichen Einstellungen zu:

1. Melden Sie sich an der AWS Management Console an.
2. Wählen Sie in der Navigationsleiste das Zahnradsymbol aus.
3. Klicken Sie auf Weitere Benutzereinstellungen, um die Seite Einheitliche Einstellungen zu öffnen.



Vereinheitlichte Einstellungen zurücksetzen

Sie können alle Unified Settings-Konfigurationen löschen und die Standardeinstellungen wiederherstellen, indem Sie Unified Settings zurücksetzen.

> **Note**
>
> Dies betrifft mehrere Bereiche AWS, darunter bevorzugte Dienste in der Navigation und im Menü „Dienste“, zuletzt besuchte Dienste in den Widgets „Startseite“ der Konsole und in den sowie alle Einstellungen AWS Console Mobile Application, die für alle Dienste gelten, wie Standardsprache, Standardregion und visueller Modus.

Um alle vereinheitlichten Einstellungen zurückzusetzen

1. Melden Sie sich an der AWS Management Console an.
2. Wählen Sie in der Navigationsleiste das Zahnradsymbol.
3. Öffnen Sie die Seite Vereinheitlichte Einstellungen, indem Sie Weitere Benutzereinstellungen auswählen.
4. Wählen Sie Alle zurücksetzen.

Einheitliche Einstellungen bearbeiten

Im folgenden Verfahren wird beschrieben, wie Sie Ihre bevorzugten Einstellungen bearbeiten.

Um vereinheitlichte Einstellungen zu bearbeiten

1. Melden Sie sich an der AWS Management Console an.
2. Wählen Sie in der Navigationsleiste das Zahnradsymbol.
3. Öffnen Sie die Seite Vereinheitlichte Einstellungen, indem Sie Weitere Benutzereinstellungen auswählen.
4. Klicken Sie auf Bearbeiten neben den gewünschten Einstellungen:

   - Lokalisierung und Standardregion:
     - Language (Sprache) ermöglicht Ihnen die Standardsprache für Konsolentext auszuwählen.
     - Default region (Standardregion) ermöglicht Ihn eine Standardregion auszuwählen, die bei jeder Anmeldung angewendet wird. Sie können jede der verfügbaren Regionen für Ihr Konto auswählen. Sie können auch die zuletzt verwendete Region als Standard auswählen.

       Weitere Informationen zum Regionen-Routing in der AWS Management Console finden Sie unter Auswahl einer Region.
   - Anzeige:
     - Unter Visual Mode (Visueller Modus) können Sie Ihre Konsole auf den Hell- oder den Dunkelmodus oder auf den Standardanzeigemodus des Browsers einstellen.

       Der Dunkelmodus ist eine Betafunktion und möglicherweise nicht für alle AWS -Servicekonsolen verfügbar.
     - Anzeige der Favoritenleiste schaltet die Anzeige der Leiste Favoriten zwischen dem vollständigen Namen des Services mit Symbol und nur dem Symbol des Services um.
     - Größe des Symbols in der Favoritenleiste schaltet die Größe des Servicesymbols in der Leiste Favoriten zwischen klein (16x16 Pixel) und groß (24x24 Pixel) um.
   - Einstellungsverwaltung:
     - Mit der Option „Zuletzt besuchte Dienste speichern“ können Sie auswählen, ob AWS Management Console Ihre zuletzt besuchten Dienste gespeichert werden sollen. Wenn Sie diese Option deaktivieren, wird auch der Verlauf der zuletzt besuchten Dienste gelöscht, sodass Sie die zuletzt besuchten Dienste nicht mehr im Servicemenü oder in den Widgets auf der Startseite der Konsole sehen. AWS Console Mobile Application

5. Wählen Sie Änderungen speichern aus.

Ändern Sie den visuellen Modus von AWS Management Console

Ihr visueller Modus stellt Ihre Konsole auf den hellen Modus, den dunklen Modus oder den Standardanzeigemodus Ihres Browsers ein.

So ändern Sie den visuellen Modus über die Navigationsleiste

1. Melden Sie sich an der AWS Management Console an.
2. Wählen Sie in der Navigationsleiste das Zahnradsymbol aus.
3. Wählen Sie für Visueller Modus Hell für den hellen Modus, Dunkel für den dunklen Modus oder Browser-Standard für den Standardanzeigemodus Ihres Browsers aus.

Ändern der Standardsprache in Unified Settings

Im folgenden Verfahren wird beschrieben, wie Sie die Standardsprache mithilfe der Navigationsleiste ändern.

So ändern Sie die Standardsprache über die Navigationsleiste

1. Melden Sie sich an der AWS Management Console an.
2. Wählen Sie in der Navigationsleiste das Zahnradsymbol aus.
3. Wählen Sie für Sprache die Option Browser-Standard oder die bevorzugte Sprache aus der Dropdown-Liste aus.

Auswählen einer Region

Für viele Dienste können Sie eine auswählen AWS-Region , die angibt, wo Ihre Ressourcen verwaltet werden. Regionen sind Gruppen von AWS Ressourcen, die sich in demselben geografischen Gebiet befinden. Sie müssen keine Region für die AWS Management Consoleoder für einige Dienste auswählen, AWS Identity and Access Management z. Weitere Informationen zu AWS-Regionen finden Sie unter Verwalten von AWS-Regionen in der Allgemeine AWS-Referenz.

So wählen Sie eine Region aus:

1. Melden Sie sich an der AWS Management Console an.

2. Wählen Sie Choose a service (Service auswählen) aus, um zur Konsole dieses Service zu wechseln.
3. Wählen Sie auf der Navigationsleiste den Namen der aktuell angezeigten Region aus. Wählen Sie anschließend die Region aus, zu der Sie wechseln möchten.

So wählen Sie eine Standardregion aus:

1. Wählen Sie in der Navigationsleiste das Einstellungen-Symbol aus und klicken Sie auf Weitere Benutzereinstellungen, um zur Seite Einheitliche Einstellungen zu navigieren.
2. Wählen Sie Bearbeiten neben Lokalisierung und Standardregion aus.
3. Wählen Sie Ihre Standardregion und dann Einstellungen speichern aus. Wenn Sie keine Standardregion auswählen, ist die letzte Region, die Sie aufgerufen haben, die Standardregion.
4. (Optional) Wähle „Gehe zu neuer Standardregion“, um sofort zu deiner neuen Standardregion zu wechseln.

> **Note**
>
> Wenn Sie AWS Ressourcen erstellt haben, diese Ressourcen aber nicht in der Konsole sehen, zeigt die Konsole möglicherweise Ressourcen aus einer anderen Region an. Einige Ressourcen, z. B. Amazon-EC2-Instances, sind für die Region spezifisch, in der sie erstellt wurden. Zur Anzeige dieser Ressourcen wählen Sie in der Regionsauswahl die Region aus, die Ihre Ressourcen enthält.

Hinzufügen und Entfernen von Favoriten

Für einen schnelleren Zugriff auf häufig verwendete Services können Sie die Konsolen dieser Services in der Liste Favoriten speichern.

So fügen Sie einen Service zur Liste Favoriten hinzu:

1. Melden Sie sich an der AWS Management Console an.
2. Wählen Sie die Schaltfläche Widgets hinzufügen oben oder unten rechts auf der Seite aus.
3. Wählen Sie im Menü Widgets hinzufügen die Option Favoriten aus, um diese der Konsole hinzuzufügen, und wählen Sie dann Hinzufügen.

Die Favoriten werden unten in Ihrer Konsolen-Startseite hinzugefügt. Sie können Favoriten per Drag-and-drop verschieben, indem Sie die Titelleiste oben am Widget auswählen und das Widget dann an einen neuen Ort auf der Seite ziehen.

4. Wählen Sie auf der Navigationsleiste Services aus.
5. Bewegen Sie in der Liste Vor kurzem aufgerufen oder in der Liste Alle Services den Mauszeiger über den Namen des Service, den Sie als Favorit hinzufügen möchten.
6. Wählen Sie den Stern links neben dem Servicenamen aus.
7. Wiederholen Sie die beiden vorherigen Schritte, um weitere Services zur Liste Favorites (Favoriten) hinzuzufügen.

So entfernen Sie einen Service aus der Liste Favoriten:

1. Wählen Sie auf der Navigationsleiste Services (Services) aus.
2. Führen Sie eine der folgenden Aktionen aus:

   - Zeigen Sie in der Liste Favoriten auf den Namen eines Services. Wählen Sie anschließend das x rechts neben dem Namen des Service aus.
   - Deaktivieren Sie in der Liste Vor kurzem aufgerufen oder in der Liste Alle Services den Stern neben dem Namen eines Service, der sich in der Liste Favoriten befindet.

Ändern des Passworts

Wenn Sie ein Kontoinhaber sind, können Sie Ihr AWS Kontopasswort über den ändern AWS Management Console.

So ändern Sie Ihr Passwort:

1. Melden Sie sich an der AWS Management Console an.
2. Wählen Sie auf der Navigationsleiste den Namen Ihres Kontos aus.
3. Wählen Sie Sicherheitsanmeldeinformationen aus.
4. Die angezeigten Optionen variieren je nach AWS-Konto Typ. Befolgen Sie anschließend die in der Konsole angezeigten Anweisungen zum Ändern des Passworts.
5. Geben Sie Ihr aktuelles Passwort einmal und das neue Passwort zweimal ein.

   Das neue Passwort muss mindestens acht Zeichen enthalten, darunter:

- Mindestens ein Symbol
- Mindestens eine Zahl
- Mindestens einen Großbuchstaben
- Mindestens einen Kleinbuchstaben

6. Wählen Sie Change password (Passwort ändern) oder Save changes (Änderungen speichern) aus.

Änderung der Sprache des AWS Management Console

Das AWS Console Home Erlebnis umfasst die Seite Unified Settings, auf der Sie die Standardsprache für AWS Dienste in der ändern können AWS Management Console. Sie können die Standardsprache auch schnell über das Einstellungsmenü ändern, auf das Sie über die Navigationsleiste zugreifen können. Sie können diese Änderung überall in der Konsole vornehmen.

> **Note**
>
> Mit diesem Verfahren wird die Sprache für die Konsole geändert, jedoch nicht für die AWS -Dokumentation. Zum Ändern der Sprache der Dokumentation verwenden Sie das Sprachmenü oben rechts auf der Seite „Dokumentation“.

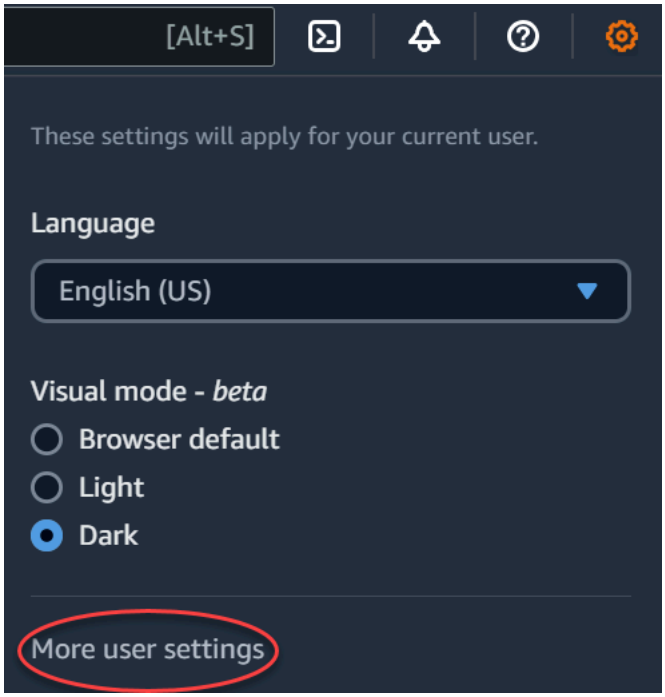
Das unterstützt AWS Management Console derzeit die folgenden Sprachen:

- Englisch (USA)
- Englisch (UK)
- Bahasa Indonesia
- Deutsch
- Französisch
- Japanisch
- Spanisch
- Italienisch
- Portugiesisch
- Koreanisch
- Chinesisch (vereinfacht)

- Chinesisch (traditionell)

So ändern Sie die Standardsprache in „Einheitliche Einstellungen“

1. Melden Sie sich an der AWS Management Console an.
2. Wählen Sie in der Navigationsleiste das Einstellungen-Symbol aus.
3. Klicken Sie auf Weitere Benutzereinstellungen, um die Seite Einheitliche Einstellungen zu öffnen.



4. In Unified Settings (Einheitliche Einstellungen), wählen Sie Edit (Bearbeiten) neben Localization and default Region (Lokalisierung und Standardregion) aus.
5. Um die Sprache auszuwählen, die für die Konsole verwendet werden soll, aktivieren Sie eine der folgenden Optionen:

   - Wählen Sie in der Dropdownliste den Standardbrowser und dann Einstellungen speichern aus.

     Der Konsolentext für alle AWS Dienste wird in Ihrer bevorzugten Sprache angezeigt, die Sie in Ihren Browsereinstellungen festgelegt haben.

     > **Note**
     >
     > Die Standardeinstellung des Browsers unterstützt nur Sprachen, die von der AWS Management Console unterstützt werden.

- Wählen Sie die bevorzugte Sprache aus der Dropdown-Liste und dann Einstellungen speichern aus.

  Der Konsolentext für alle AWS Dienste wird in Ihrer bevorzugten Sprache angezeigt.

So ändern Sie die Standardsprache über die Navigationsleiste

1. Melden Sie sich an der AWS Management Console an.
2. Wählen Sie in der Navigationsleiste das Einstellungen-Symbol aus.
3. Wählen Sie für Sprache entweder die Option Browser-Standard oder die bevorzugte Sprache aus der Dropdown-Liste aus.

Erste Schritte mit einem Service

Die AWS Management Console bietet mehrere Methoden für die Navigation zu einzelnen Servicekonsolen.

So öffnen Sie eine Konsole für einen Service

Führen Sie eine der folgenden Aktionen aus:

- Geben Sie in das Suchfeld in der Navigationsleiste den Namen des Services ganz oder teilweise ein. Wählen Sie dann unter Services den gewünschten Service in der Liste der Suchergebnisse aus. Weitere Informationen finden Sie unter Mit Unified Search nach Produkten, Dienstleistungen, Funktionen und mehr suchen.
- Unter Recently visited services (Kürzlich besuchte Services) wählen Sie einen Servicenamen aus.
- Unter Recently visited services (Kürzlich besuchte Services) Widget, wählen Sie View all (Alle ansehen) AWS-Services aus. Wählen Sie dann auf der Seite All (Alle) AWS-Services, einen Servicenamen aus.
- Wählen Sie in der Navigationsleiste Services aus, um eine vollständige Liste der Services zu öffnen. Wählen Sie unter Kürzliche besuchte Services oder Alle Services einen Servicenamen aus.

Mit Unified Search nach Produkten, Dienstleistungen, Funktionen und mehr suchen

Das Suchfeld in der Navigationsleiste bietet ein einheitliches Suchwerkzeug zum Auffinden von AWS -Services und -Funktionen, Service-Dokumentation und AWS Marketplace. Geben Sie einfach ein paar Buchstaben ein, um Ergebnisse aus all diesen Kategorien zu sehen. Je mehr Buchstaben Sie eingeben, desto mehr werden Ihre Ergebnisse verfeinert.

Um nach einem Service, einer Funktion, einer Dokumentation oder einem AWS Marketplace Produkt zu suchen

1. Geben Sie in das Suchfeld in der AWS Management Console Navigationsleiste von alle oder einen Teil Ihrer Suchbegriffe ein.
2. Führen Sie einen der folgenden Schritte aus, um die Suche zu verfeinern und mehr Details zu erhalten:
   - Um die Ergebnisse auf den gewünschten Inhaltstyp einzugrenzen, wählen Sie eine der Kategorien auf der linken Seite aus.
   - Um weitere Ergebnisse für eine bestimmte Kategorie anzuzeigen, wählen Sie Alle ***n*** Ergebnisse nach jeder Kategorieüberschrift aus. Wählen Sie in der oberen linken Ecke Zurück aus, um zu den Hauptergebnissen zurückzukehren.
   - Um schnell zu beliebten Funktionen eines Services zu navigieren, halten Sie den Servicenamen in den Ergebnissen an und wählen Sie einen Link aus.
   - Um weitere Informationen zu einer Dokumentation oder einem AWS Marketplace Ergebnis zu erhalten, halten Sie den Mauszeiger auf dem Titel des Ergebnisses.
3. Wählen Sie einen beliebigen Link aus, um zu Ihrem gewünschten Service, Thema oder AWS Marketplace zu navigieren.

> **Tip**
>
> Sie können auch Ihre Tastatur verwenden, um schnell zum obersten Suchergebnis zu navigieren. Drücken Sie zuerst Alt+S (Windows) oder Option+S (macOS), um auf die Suchleiste zuzugreifen. Beginnen Sie dann mit der Eingabe Ihres Suchbegriffs. Drücken Sie die Eingabetaste, wenn das gewünschte Ergebnis am Anfang der Liste angezeigt wird.

Geben Sie beispielsweise ec2 ein und drücken Sie die Eingabetaste, um schnell zu Amazon EC2-Konsole zu navigieren.

Chatten Sie mit Amazon Q Developer

Amazon Q Developer ist ein auf generativer künstlicher Intelligenz (KI) basierender Konversationsassistent, der Ihnen helfen kann, AWS Anwendungen zu verstehen, zu erstellen, zu erweitern und zu betreiben. Sie können Amazon Q alle Fragen stellen AWS, einschließlich Fragen zur AWS Architektur, Ihren AWS Ressourcen, bewährten Methoden, Dokumentation und mehr. Sie können auch Supportanfragen erstellen und Unterstützung von einem Live-Mitarbeiter erhalten. Weitere Informationen finden Sie unter Was ist Amazon Q? im Amazon Q Developer User Guide.

Erste Schritte mit Amazon Q

Sie können den Chat mit Amazon Q auf den AWS Dokumentationswebsites AWS Management Console, AWS Websites oder in der AWS Console Mobile Application beginnen, indem Sie das sechseckige Amazon Q-Symbol auswählen. Weitere Informationen finden Sie unter Erste Schritte mit Amazon Q Developer im Amazon Q Developer User Guide.

Beispielfragen

Im Folgenden finden Sie einige Beispielfragen, die Sie Amazon Q stellen können:

- `How do I get billing support?`
- `How do I create an EC2 instance?`
- `How do I troubleshoot a "Failed to load" error?`
- `How do I close an AWS account?`
- `Can you connect me with a person?`

Worauf AWS läuft MyApplications?

myApplications ist eine Erweiterung von Console Home, mit der Sie die Kosten, den Zustand, den Sicherheitsstatus und die Leistung Ihrer Anwendungen in AWS verwalten und überwachen können. Sie können auf alle Anwendungen in Ihrem Konto, wichtige Kennzahlen für alle Anwendungen und einen Überblick über Kosten-, Sicherheits- und Betriebsmetriken sowie Erkenntnisse aus mehreren Servicekonsolen von einer Ansicht aus zugreifen AWS Management Console. MyApplications umfasst Folgendes:

- Das Widget „Anwendungen“ auf der Startseite der Konsole
- myApplications, mit dem Sie die Kosten für Anwendungsressourcen und Sicherheitsergebnisse einsehen können
- Das myApplications-Dashboard, das einen Überblick über wichtige Anwendungsmetriken wie Kosten, Leistung und Sicherheitsdaten bietet

Features von myApplications

- Anwendungen erstellen – erstellen Sie neue Anwendungen und organisieren Sie deren Ressourcen. Ihre Anwendungen werden automatisch in MyApplications angezeigt, sodass Sie in den APIs AWS Management Console, CLI und SDKs Maßnahmen ergreifen können. Infrastructure as Code (IaC) wird generiert, wenn Sie eine Anwendung erstellen, und ist über das myApplication-Dashboard zugänglich. IaC kann in IaC-Tools wie Terraform verwendet werden. AWS CloudFormation
- Auf Ihre Anwendungen zugreifen – Sie können über das myApplications-Widget schnell auf jede Ihrer Anwendungen zugreifen, indem Sie sie auswählen.
- Anwendungsmetriken vergleichen – verwenden Sie myApplications, um wichtige Metriken für Anwendungen wie die Kosten für Anwendungsressourcen und die Anzahl kritischer Sicherheitsergebnisse für mehrere Anwendungen zu vergleichen.
- Anwendungen überwachen und verwalten — Beurteilen Sie den Zustand und die Leistung von Anwendungen anhand von Alarmen, Kanarien und Service-Level-Zielvorgaben Amazon CloudWatch, Ergebnissen und Kostentrends von AWS Security Hub. AWS Cost Explorer Service Unter finden Sie auch Zusammenfassungen und Optimierungen von Berechnungsmetriken sowie die Verwaltung der Einhaltung von Ressourcenbestimmungen und des Konfigurationsstatus. AWS Systems Manager

Zugehörige Services

myApplications verwendet die folgenden Services:

- AppRegistry
- AppManager
- Amazon CloudWatch
- Amazon EC2
- AWS Lambda
- AWS Ressourcen Explorer
- AWS Security Hub
- Systems Manager
- AWS Service Catalog
- Tagging

Zugreifen auf myApplications

Sie können auf myApplications von der AWS Management Console aus zugreifen, indem Sie in der linken Seitenleiste myApplications auswählen.

Preisgestaltung

MyApplications on AWS wird ohne zusätzliche Kosten angeboten. Es fallen keine Einrichtungsgebühren oder Vorableistungen an. Die Nutzungsgebühren für die zugrunde liegenden Ressourcen und Services, die im myApplication-Dashboard zusammengefasst sind, fallen weiterhin zu den für diese Ressourcen veröffentlichten Tarifen an.

Unterstützte Regionen

MyApplications ist in den folgenden Sprachen verfügbar: AWS-Regionen

- US East (Ohio)
- USA Ost (Nord-Virginia)

- USA West (Nordkalifornien)
- USA West (Oregon)
- Asien-Pazifik (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Europe (Frankfurt)
- Europa (Irland)
- Europe (London)
- Europe (Paris)
- Europa (Stockholm)
- Südamerika (São Paulo)

Opt-In-Regionen

Opt-In-Region sind nicht standardmäßig aktiviert. Sie müssen diese Regionen manuell aktivieren, um sie mit myApplications verwenden zu können. Weitere Informationen zu finden Sie AWS-Regionen unter Verwalten AWS-Regionen. Die folgenden Opt-in-Regionen werden unterstützt:

- Afrika (Kapstadt)
- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Melbourne)
- Europa (Milan)
- Europa (Spain)
- Europa (Zürich)
- Naher Osten (Bahrain)

- Naher Osten (VAE)
- Israel (Tel Aviv)

Erste Schritte mit myApplications

Gehen Sie bei den ersten Schritten mit myApplications wie folgt vor, um Ihre Anwendungen zu erstellen, zu überwachen und zu verwalten.

Schritt 1: Erstellen einer -Anwendung

Erstellen Sie eine neue Anwendung oder integrieren Sie eine bestehende AppRegistry Anwendung, die vor dem 8. November 2023 erstellt wurde, um mit MyApplications zu beginnen.

Create an application

So erstellen Sie eine Anwendung

1. Melden Sie sich an der AWS Management Console an.
2. Wählen Sie in der linken Seitenleiste myApplications aus.
3. Wählen Sie Create application aus.
4. Geben Sie einen Anwendungsnamen ein.
5. (Optional) Geben Sie eine Anwendungsbeschreibung ein.
6. (Optional) Fügen Sie Tags hinzu. Tags sind Schlüssel-Wert-Paare, die auf Ressourcen angewendet werden, um Metadaten zu diesen Ressourcen zu enthalten.

   > **Note**
   >
   > Das AWS Anwendungs-Tag wird automatisch auf neu erstellte Anwendungen angewendet und kann verwendet werden, um Ressourcen zu identifizieren, die mit Ihrer Anwendung verknüpft sind. Weitere Informationen finden Sie im AWS Service Catalog AppRegistry Administratorhandbuch unter Das AWS Anwendungs-Tag.

7. (Optional) Fügen Sie Attributgruppen hinzu. Sie können mit Attributgruppen Anwendungsmetadaten speichern.
8. Wählen Sie Weiter aus.
9. (Optional) Fügen Sie vorhandene Ressourcen hinzu:

> **Note**
>
> Wenn Sie nach Ressourcen suchen und diese hinzufügen möchten, müssen Sie AWS Ressourcen Explorer aktivieren. Weitere Informationen finden Sie unter Erste Schritte mit AWS Ressourcen Explorer.
> Alle hinzugefügten Ressourcen sind mit dem AWS Anwendungs-Tag gekennzeichnet.

a. Wählen Sie Ressourcen auswählen aus.

b. (Optional) Wählen Sie eine Ansicht aus.

c. Suchen Sie nach Ihren Ressourcen. Sie können nach Schlüsselwörtern, Namen oder Typ suchen oder einen Ressourcentyp auswählen.

> **Note**
>
> Wenn Sie die gesuchte Ressource nicht finden können, beheben Sie das Problem mit AWS Ressourcen Explorer. Weitere Informationen finden Sie unter Problembehandlung bei Resource Explorer-Suchproblemen im Resource-Explorer-Benutzerhandbuch.

d. Aktivieren Sie das Kontrollkästchen neben den Benutzern, die Sie hinzufügen möchten.

e. Wählen Sie Hinzufügen aus.

f. Wählen Sie Weiter aus.

10. Überprüfen Sie Ihre Auswahl.

11. Wenn Sie einen AWS CloudFormation Stapel zuordnen möchten, aktivieren Sie das Kontrollkästchen unten auf der Seite.

> **Note**
>
> Das Hinzufügen eines AWS CloudFormation Stacks zur Anwendung erfordert ein Stack-Update, da alle Ihrer Anwendung hinzugefügten Ressourcen mit dem AWS Anwendungs-Tag gekennzeichnet sind. Manuelle Konfigurationen, die nach der letzten Aktualisierung des Stacks durchgeführt wurden, werden nach diesem Update möglicherweise nicht mehr berücksichtigt. Dies kann zu Ausfallzeiten oder anderen

Anwendungsproblemen führen. Weitere Informationen finden Sie unter Aktualisieren von Verhalten von Stack-Ressourcen im AWS CloudFormation -Benutzerhandbuch.

12. Wählen Sie Create application aus.

Onboard existing application

Um eine bestehende AppRegistry Anwendung zu integrieren

1. Melden Sie sich an der AWS Management Console an.
2. Wählen Sie in der linken Seitenleiste myApplications aus.
3. Verwenden Sie die Suchleiste, um nach Ihrer Anwendung zu suchen.
4. Wählen Sie Ihre Anwendung aus.
5. Wählen Sie den Onboarding für ***Anwendungsnamen*** ausführen aus.
6. Wenn Sie einen CloudFormation Stapel zuordnen möchten, aktivieren Sie das Kontrollkästchen im Warnfeld.
7. Wählen Sie Onboarding für Anwendung ausführen aus.

Schritt 2: Anzeigen von Anwendungen

Sie können Ihre Anwendungen in allen Regionen oder bestimmten Regionen und die entsprechenden Informationen in einer Karten- oder Tabellenansicht anzeigen.

So zeigen Sie Anwendungen an

1. Wählen Sie in der linken Seitenleiste myApplications aus.
2. Wählen Sie unter Regionen die Option Aktuelle Region oder Unterstützte Regionen aus.
3. Wenn Sie nach einer bestimmten Anwendung suchen, geben Sie deren Namen, die Suchwörter oder die Beschreibung in die Suchleiste ein.
4. (Optional) Ihre Standardansicht ist die Kartenansicht. So passen Sie Ihre Anwendungsseite an:
   a. Wählen Sie das Zahnradsymbol aus.
   b. (Optional) Wählen Sie die Seitengröße aus.
   c. (Optional) Wählen Sie die Karten- oder Tabellenansicht aus.
   d. (Optional) Wählen Sie die Seitengröße aus.

e. (Optional) Wenn Sie die Tabellenansicht verwenden, wählen Sie die Eigenschaften für die Tabellenansicht aus.

f. (Optional) Schalten Sie ein, welche Anwendungseigenschaften sichtbar sind und in welcher Reihenfolge sie angezeigt werden.

g. Wählen Sie Bestätigen aus.

Verwalten von Anwendungen

In diesem Thema wird beschrieben, wie Sie Ihre Anwendungen verwalten können.

Bearbeiten von Anwendungen

Die Bearbeitung Ihrer Anwendung wird geöffnet AppRegistry , sodass Sie ihre Beschreibung aktualisieren können. Sie können es auch verwenden AppRegistry , um die Tags und Attributgruppen Ihrer Anwendung zu bearbeiten.

So bearbeiten Sie eine Anwendung

1. Öffnen Sie die AWS Management Console.
2. Wählen Sie in der linken Seitenleiste der Konsole myApplications aus.
3. Wählen Sie die Anwendung aus, die Sie bearbeiten möchten.
4. Wählen Sie im myApplication-Dashboard die Option Aktionen und dann Anwendung bearbeiten aus.
5. Aktualisieren Sie die Beschreibung unter Anwendungsbeschreibung bearbeiten und wählen Sie dann Änderungen speichern aus.

So bearbeiten Sie Tags

- Folgen Sie den Schritten unter Tags verwalten im AWS Service Catalog AppRegistry Administratorhandbuch.

So bearbeiten Sie Attributgruppen

- Folgen Sie den Schritten unter Attributgruppen bearbeiten im AWS Service Catalog AppRegistry Administratorhandbuch.

Löschen von Anwendungen

Sie können Anwendungen löschen, wenn sie nicht mehr benötigt werden.

So löschen Sie eine Anwendung

1. Öffnen Sie die AWS Management Console.
2. Wählen Sie in der linken Seitenleiste der Konsole myApplications aus.
3. Wählen Sie die Anwendung aus, die Sie löschen möchten.
4. Wählen Sie im myApplication-Dashboard die Option Aktionen aus.
5. Klicken Sie auf Delete Application (Anwendung löschen).
6. Wählen Sie Löschen aus.
7. Bestätigen Sie die Löschung und wählen Sie dann Anwendung löschen aus.

Erstellen von Codeausschnitten

myApplications erstellt Codeausschnitte für all Ihre Anwendungen. Sie können mit Codeausschnitten einer Anwendung mithilfe der Tools für Infrastructure as Code (IaC) automatisch neu erstellte Ressourcen hinzuzufügen. Alle hinzugefügten Ressourcen sind mit dem AWS Anwendungs-Tag gekennzeichnet, um sie Ihrer Anwendung zuzuordnen.

So erstellen Sie einen Codeausschnitt für Ihre Anwendung

1. Öffnen Sie die AWS Management Console.
2. Wählen Sie in der linken Seitenleiste der Konsole myApplications aus.
3. Suchen Sie nach einer Anwendung und wählen Sie sie aus.
4. Wählen Sie Aktionen.
5. Wählen Sie Codeausschnitt abrufen aus.
6. Wählen Sie einen Codeausschnittstyp aus.
7. Wählen Sie Kopieren aus, um die Nachricht in die Zwischenablage zu kopieren.
8. Fügen Sie Ihren Code in Ihr IaC-Tool ein.

Verwalten von Ressourcen

In diesem Thema wird beschrieben, wie Sie Ihre Ressourcen verwalten.

Hinzufügen von Ressourcen

Durch das Hinzufügen von Ressourcen zu Ihren Anwendungen können Sie diese gruppieren und ihre Sicherheit, Leistung und Konformität verwalten.

So fügen Sie Ressourcen hinzu

1. Öffnen Sie die AWS Management Console.
2. Wählen Sie in der linken Seitenleiste der Konsole myApplications aus.
3. Suchen Sie nach einer Anwendung und wählen Sie sie aus.
4. Wählen Sie Ressourcen verwalten aus.
5. Wählen Sie Ressourcen hinzufügen aus.
6. (Optional) Wählen Sie eine Ansicht aus.
7. Suchen Sie nach Ihren Ressourcen. Sie können nach Schlüsselwörtern, Namen oder Typ suchen oder einen Ressourcentyp auswählen.

   > **Note**
   >
   > Wenn Sie die gesuchte Ressource nicht finden können, beheben Sie das Problem mit AWS Ressourcen Explorer. Weitere Informationen finden Sie unter Problembehandlung bei Resource Explorer-Suchproblemen im Resource-Explorer-Benutzerhandbuch.

8. Aktivieren Sie das Kontrollkästchen neben den Benutzern, die Sie hinzufügen möchten.
9. Wählen Sie Hinzufügen aus.

Entfernen von Ressourcen

Sie können Ressourcen entfernen, um die Zuordnung zu Ihrer Anwendung aufzuheben.

So entfernen Sie Ressourcen

1. Öffnen Sie die AWS Management Console.
2. Wählen Sie in der linken Seitenleiste der Konsole myApplications aus.
3. Suchen Sie nach einer Anwendung und wählen Sie sie aus.
4. Wählen Sie Ressourcen verwalten aus.
5. (Optional) Wählen Sie eine Ansicht aus.

6. Suchen Sie nach Ihren Ressourcen. Sie können nach Schlüsselwörtern, Namen oder Typ suchen oder einen Ressourcentyp auswählen.

> **Note**
>
> Wenn Sie die gesuchte Ressource nicht finden können, beheben Sie das Problem mit AWS Ressourcen Explorer. Weitere Informationen finden Sie unter Problembehandlung bei Resource Explorer-Suchproblemen im Resource-Explorer-Benutzerhandbuch.

7. Wählen Sie Remove (Entfernen) aus.
8. Bestätigen Sie, dass Sie die Ressource entfernen möchten, indem Sie Ressourcen entfernen auswählen.

myApplications-Dashboard

Jede Anwendung, die Sie erstellen oder integrieren, hat ihr eigenes myApplications-Dashboard. Das MyApplications-Dashboard enthält Widgets für Kosten, Sicherheit und Betrieb, die Einblicke aus verschiedenen AWS Diensten bieten. Jedes Widget kann auch als Favorit markiert, neu angeordnet, entfernt oder in der Größe geändert werden. Weitere Informationen finden Sie unter Arbeiten mit Widgets.

Widget zur Einrichtung des Anwendungs-Dashboards

Dieses Widget enthält eine Liste mit empfohlenen Einstiegsaktivitäten, die Sie bei der Konfiguration AWS-Services der Verwaltung von Anwendungsressourcen verwenden können.

Widget mit der Zusammenfassung der Anwendung

Dieses Widget zeigt den Namen, die Beschreibung und das AWS Anwendungs-Tag für Ihre Anwendung an. Sie können in Infrastructure as Code (IAC) auf das Anwendungs-Tag zugreifen und es kopieren, um Ressourcen manuell zu markieren.

Computing-Widget

Dieses Widget zeigt Informationen und Metriken für Computing-Ressourcen an, die Sie Ihrer Anwendung hinzufügen. Dazu gehören die Gesamtzahl der Alarme und die Gesamtzahl der Computing-Ressourcentypen. Das Widget zeigt auch Trenddiagramme zur

Ressourcenleistungsmetrik Amazon CloudWatch für die CPU-Auslastung von Amazon EC2 EC2-Instances und Lambda-Aufrufe.

Konfigurieren des Computing-Widgets

Wenn Sie Daten im Computing-Widget auffüllen möchten, richten Sie mindestens eine Amazon-EC2-Instance oder eine Lambda-Funktion für Ihre Anwendung ein. Weitere Informationen finden Sie in der Dokumentation für Amazon Elastic Compute Cloud und Erste Schritte mit Lambda im AWS Lambda - Entwicklerhandbuch.

Kosten- und Nutzungs-Widget

Dieses Widget zeigt AWS Kosten- und Nutzungsdaten für Ihre Anwendungsressourcen. Sie können diese Daten verwenden, um die monatlichen Kosten zu vergleichen und die Aufschlüsselung der Kosten nach AWS-Service einzusehen. Dieses Widget fasst nur die Kosten für Ressourcen zusammen, die mit dem AWS Anwendungs-Tag gekennzeichnet sind, ohne Steuern, Gebühren und andere gemeinsame Kosten, die nicht direkt mit einer Ressource verknüpft sind. Die angegebenen Kosten sind nicht kombiniert und werden mindestens einmal alle 24 Stunden aktualisiert. Weitere Informationen dazu finden Sie unter Analysieren Ihrer Kosten mit AWS Ressourcen Explorer im AWS Cost Management -Benutzerhandbuch.

Konfigurieren des Widgets für Kosten- und Nutzung

Um das Widget „Kosten und Nutzung“ zu konfigurieren, aktivieren Sie es AWS Cost Explorer Service für Ihre Anwendung und Ihr Konto. Dieser Service wird ohne zusätzliche Kosten angeboten und es fallen keine Einrichtungsgebühren oder Vorabverpflichtungen an. Weitere Informationen finden Sie unter Aktivieren von Cost Explorer im AWS Cost Management -Benutzerhandbuch.

AWS Sicherheits-Widget

Dieses Widget zeigt die Sicherheitsergebnisse von AWS Security für Ihre Anwendung an. AWS Sicherheit bietet einen umfassenden Überblick über die Sicherheitsergebnisse für Ihre Anwendung in AWS. Sie können auf aktuelle Erkenntnisse mit Priorität nach Schweregrad zugreifen, deren Sicherheitsstatus überwachen, auf aktuelle Erkenntnisse mit kritischem oder hohem Schweregrad zugreifen und Erkenntnisse für nächste Schritte gewinnen. Weitere Informationen finden Sie unter AWS Security Hub.

Konfiguration des AWS Sicherheits-Widgets

Um das AWS Sicherheits-Widget zu konfigurieren, richten Sie es AWS Security Hub für Ihre Anwendung und Ihr Konto ein. Weitere Informationen finden Sie unter Was ist AWS Security Hub? im AWS Security Hub Benutzerhandbuch. Preisinformationen finden Sie im AWS Security Hub - Benutzerhandbuch unter Kostenlose AWS Security Hub -Testversion, -Nutzung und -Preise.

AWS Security Hub erfordert die Konfiguration von AWS Config Recording. Dieser Service bietet eine detaillierte Ansicht der mit Ihrem AWS Konto verknüpften Ressourcen. Weitere Informationen finden Sie unter AWS Systems Manager im AWS Systems Manager -Benutzerhandbuch.

DevOps Widget

Dieses Widget zeigt betriebliche Erkenntnisse, sodass Sie die Compliance bewerten und Maßnahmen für Ihre Anwendung ergreifen können. Zu diesen Erkenntnissen gehören:

- Flottenverwaltung
- Statusverwaltung
- Patch-Management
- Konfiguration und OpsItems Verwaltung

Konfiguration des DevOps Widgets

Um das DevOps Widget zu konfigurieren, aktivieren Sie es AWS Systems Manager OpsCenter für Ihre Anwendung und Ihr Konto. Weitere Informationen finden Sie unter Erste Schritte mit Systems Manager Explorer und OpsCenter im AWS Systems Manager Benutzerhandbuch. OpsCenter Durch die Aktivierung können AWS Systems Manager Explorer sie konfiguriert AWS Config werden, Amazon CloudWatch sodass ihre Ereignisse automatisch auf der OpsItems Grundlage häufig verwendeter Regeln und Ereignisse erstellt werden. Weitere Informationen finden Sie OpsCenter im AWS Systems Manager Benutzerhandbuch unter Einrichtung.

Sie können Ihre Instances so konfigurieren, dass Systems-Manager-Agenten ausgeführt werden, und Berechtigungen anwenden, um die Patch-Suche zu aktivieren. Weitere Informationen finden Sie unter AWS Systems Manager Quick Setup im AWS Systems Manager -Benutzerhandbuch.

Sie können auch automatisiertes Patchen von Amazon EC2 EC2-Instances für Ihre Anwendung einrichten, indem Sie AWS Systems Manager Patch Manager einrichten. Weitere Informationen finden Sie unter Quick Setup von Patch-Richtlinien im AWS Systems Manager -Benutzerhandbuch.

Preisinformationen finden Sie unter AWS Systems Manager Preise.

Widget für Überwachung und Betrieb

Dieses Widget zeigt:

- Alarme und Benachrichtigungen für Ressourcen, die mit Ihrer Anwendung verknüpft sind
- Service Level Objectives (SLOs) und Metriken für Anwendungen
- Verfügbare Messwerte für AWS Application Signals

Konfigurieren des Widgets für Überwachung und Betrieb

Um das Widget „Überwachung und Betrieb“ zu konfigurieren, müssen Sie in Ihrem AWS Konto CloudWatch Alarme und Kanarien erstellen. Weitere Informationen finden Sie unter Verwenden von CloudWatch Amazon-Alarmen und Erstellen eines Kanarienvogels im CloudWatch Amazon-Benutzerhandbuch. Die Preise für CloudWatch Alarm und Synthetic Canary finden Sie unter CloudWatch Amazon-Preise bzw. im AWS Cloud Operations and Migrations Blog.

Weitere Informationen zu CloudWatch Application Signals finden Sie unter Enable Amazon CloudWatch Application Insights im CloudWatch Amazon-Benutzerhandbuch.

Tags-Widget

Dieses Widget zeigt alle mit Ihrer Anwendung verknüpften Tags an. Sie können mit diesem Widget Anwendungsmetadaten (Kritikalität, Umgebung, Kostenstelle) verfolgen und verwalten. Weitere Informationen finden Sie unter Was sind Tags? im AWS Whitepaper Bewährte Methoden zum Kennzeichnen von AWS Ressourcen.

AWS Management Console Privater Zugang

AWS Management Console Private Access ist eine erweiterte Sicherheitsfunktion zur Steuerung des Zugriffs auf. AWS Management Console AWS Management Console Private Access ist nützlich, wenn Sie verhindern möchten, dass sich Benutzer unerwartet AWS-Konten von Ihrem Netzwerk aus anmelden. Mit dieser Funktion können Sie den AWS Management Console Zugriff auf bestimmte Daten beschränken, von AWS-Konten denen bekannt ist, wann der Datenverkehr aus Ihrem Netzwerk stammt.

Themen

AWS-Regionen Unterstützte Servicekonsolen und Funktionen

AWS Management Console Private Access unterstützt nur einen Teil der Regionen und AWS Dienste. Nicht unterstützte Servicekonsolen werden in der AWS Management Console inaktiv sein. Darüber hinaus können bestimmte AWS Management Console Funktionen deaktiviert sein, wenn Sie AWS Management Console Private Access verwenden, z. B. die Auswahl der Standardregion in den Unified Settings.

Die folgenden Regionen und Servicekonsolen werden unterstützt.

Unterstützte Regionen

- US East (Ohio)
- USA Ost (Nord-Virginia)
- USA West (Nordkalifornien)
- USA West (Oregon)

- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Seoul)
- Asien-Pazifik (Osaka)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Europe (Frankfurt)
- Europa (Irland)
- Europe (London)
- Europe (Paris)
- Europa (Stockholm)
- Südamerika (São Paulo)
- Afrika (Kapstadt)
- Asia Pacific (Hongkong)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Melbourne)
- Kanada West (Calgary)
- Europa (Milan)
- Europa (Spain)
- Europa (Zürich)
- Naher Osten (Bahrain)
- Naher Osten (VAE)
- Israel (Tel Aviv)

Unterstützte Servicekonsolen

- Amazon API Gateway
- AWS App Mesh

- AWS Application Migration Service
- Amazon Athena
- AWS Auto Scaling
- AWS Billing Conductor
- AWS Certificate Manager
- AWS Cloud Map
- Amazon CloudFront
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- Amazon CodeGuru
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Compute Optimizer
- AWS Console Home
- AWS Database Migration Service
- AWS DeepRacer
- Amazon DocumentDB
- Amazon-DynamoDB
- Amazon EC2
- Amazon EC2 Global View
- EC2 Image Builder
- Amazon EC2 Instance Connect
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- AWS Elastic Disaster Recovery
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache

- Amazon EMR
- Amazon EventBridge
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station
- Amazon GuardDuty
- AWS Identity and Access Management
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- Amazon Kendra
- AWS Key Management Service
- Amazon Kinesis
- Amazon Managed Service für Apache Flink
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Managed Grafana
- Amazon Managed Streaming für Apache Kafka
- Amazon Managed Workflows for Apache Airflow (MWAA)
- Strategieempfehlungen für den AWS Migration Hub
- Amazon MQ
- Network Access Analyzer
- AWS Network Manager
- OpenSearch Amazon-Dienst
- AWS Organizations
- Amazon S3 in Outposts
- Amazon SageMaker Runtime

- SageMaker Synthetische Amazon-Daten
- AWS Secrets Manager
- Service Quotas
- AWS Signer
- Amazon Simple Email Service
- Amazon Simple Queue Service
- Amazon-Simple-Storage-Service (Amazon-S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Support
- AWS Systems Manager
- AWS Transfer Family
- Einheitliche Einstellungen
- Amazon VPC IP Address Manager

Überblick über die Sicherheitskontrollen von AWS Management Console Private Access

Kontobeschränkungen für die AWS Management Console von Ihrem Netzwerk aus

AWS Management Console Private Access ist in Szenarien nützlich, in denen Sie den Zugriff auf das AWS Management Console von Ihrem Netzwerk aus auf eine bestimmte Gruppe von AWS-Konten in Ihrer Organisation bekannten Daten beschränken möchten. Auf diese Weise können Sie verhindern, dass sich Benutzer in Ihrem Netzwerk bei unerwarteten AWS-Konten anmelden. Sie können diese Kontrollen mithilfe der AWS Management Console VPC-Endpunktrichtlinie implementieren. Weitere Informationen finden Sie unter Implementieren von Service-Kontrollrichtlinien und von VPC-Endpunktrichtlinien.

Konnektivität von Ihrem Netzwerk zum Internet

Für den Zugriff auf Ressourcen, die von verwendet werden AWS Management Console, wie z. B. statische Inhalte (CSS, Bilder)JavaScript, ist weiterhin eine Internetverbindung von Ihrem

Netzwerk aus erforderlich, die alle AWS-Services nicht aktiviert sind AWS PrivateLink. Eine Liste der Top-Level-Domains, die von der verwendet werden AWS Management Console, finden Sie unterFehlerbehebung.

> **Note**
>
> Derzeit unterstützt AWS Management Console Private Access keine Endpunkte wie `status.aws.amazon.comhealth.aws.amazon.com`, und. `docs.aws.amazon.com` Sie müssen diese Domains an das öffentliche Internet weiterleiten.

Erforderliche VPC-Endpunkte und DNS-Konfiguration

AWS Management Console Für Private Access sind die folgenden zwei VPC-Endpunkte pro Region erforderlich. Ersetzen Sie die *`Region`* durch Ihre eigenen Regioneninformationen.

1. com.amazonaws. *`region .console`* für AWS Management Console
2. com.amazonaws. *`region. Melden`* Sie sich an für AWS-Anmeldung

> **Note**
>
> Geben Sie immer die Infrastruktur und Netzwerkkonnektivität für die Region USA Ost (Nord-Virginia) (us-east-1) an, unabhängig davon, welche anderen Regionen Sie für die AWS Management Console verwenden. Sie können AWS Transit Gateway verwenden, um die Konnektivität zwischen USA Ost (Nord-Virginia) und allen anderen Regionen einzurichten. Weitere Informationen finden Sie unter Erste Schritte mit Transit Gateways im Amazon VPC Transit Gateways-Handbuch. Sie können auch Amazon VPC Peering verwenden. Weitere Informationen finden Sie unter Was ist VPC Peering? im Amazon VPC Peering-Handbuch. Einen Vergleich dieser Optionen finden Sie unter Amazon VPC-zu-Amazon VPC-Anbindungsoptionen im Whitepaper Optionen für Verbindungen der Amazon Virtual Private Cloud.

DNSKonfiguration für und AWS Management ConsoleAWS-Anmeldung

Um Ihren Netzwerkverkehr an die jeweiligen VPC-Endpunkte weiterzuleiten, konfigurieren Sie DNS-Datensätze in dem Netzwerk, von dem aus Ihre Benutzer auf die AWS Management Console

zugreifen. Diese DNS-Datensätze leiten den Browserverkehr Ihrer Benutzer zu den von Ihnen erstellten VPC-Endpunkten weiter.

Sie können eine einzelne gehostete Zone erstellen. Endpunkte wie `health.aws.amazon.com` und `docs.aws.amazon.com` werden jedoch nicht zugänglich sein, da sie keine VPC-Endpunkte haben. Sie müssen diese Domains an das öffentliche Internet weiterleiten. Wir empfehlen, zwei private gehostete Zonen pro Region zu erstellen, eine für `signin.aws.amazon.com` und eine für `console.aws.amazon.com` mit den folgenden CNAME-Datensätzen:

- Regionale CNAME-Datensätze (in allen Regionen)
- region.signin.aws.amazon.com zeigt auf den VPC-Endpunkt in der Anmeldezone AWS-Anmeldung DNS
- region.console.aws.amazon.com zeigt auf den VPC-Endpunkt in der Konsolenzone AWS Management Console DNS
- Regionslose CNAME-Datensätze nur für die Region USA Ost (Nord-Virginia). Sie müssen immer die Region US East (Nord-Virginia) einrichten.
  - signin.aws.amazon.com zeigt auf den AWS-Anmeldung VPC-Endpunkt in USA Ost (Nord-Virginia) (us-east-1)
  - console.aws.amazon.com zeigt auf den AWS Management Console VPC-Endpunkt in USA Ost (Nord-Virginia) (us-east-1)

Anweisungen zum Erstellen eines CNAME-Datensatzes finden Sie unter Arbeiten mit Datensätzen im Amazon Route 53-Entwicklerhandbuch.

Einige AWS Konsolen, darunter Amazon S3, verwenden unterschiedliche Muster für ihre DNS Namen. Nachfolgend finden Sie zwei Beispiele:

- support.console.aws.amazon.com
- s3.console.aws.amazon.com

Um diesen Traffic an Ihren AWS Management Console VPC-Endpunkt weiterleiten zu können, müssen Sie diese Namen einzeln hinzufügen. Wir empfehlen Ihnen, das Routing für alle Endgeräte zu konfigurieren, um ein vollständig privates Erlebnis zu gewährleisten. Dies ist jedoch nicht erforderlich, um AWS Management Console Private Access zu verwenden.

Die folgenden `json` Dateien enthalten die vollständige Liste der AWS-Service Endpunkte und Konsolenendpunkte, die pro Region konfiguriert werden müssen. Verwenden Sie das

`PrivateIpv4DnsNames`-Feld unter dem `com.amazonaws.`*`region`*`.console`-Endpunkt für die DNS-Namen.

- https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
- https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
- https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json
- https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/il-central-1.config.json

> **Note**
>
> Diese Liste wird jeden Monat aktualisiert, wenn wir AWS Management Console Private Access weitere Endpunkte hinzufügen. Um Ihre privat gehosteten Zonen auf dem neuesten Stand zu halten, rufen Sie regelmäßig die vorherige Dateiliste ab.

Wenn Sie Route 53 verwenden, um Ihre DNS zu konfigurieren, gehen Sie zu https://console.aws.amazon.com/route53/v2/hostedzones #, um die DNS-Einrichtung zu überprüfen. Stellen Sie für jede private gehostete Zone in Route 53 sicher, dass die folgenden Datensätze vorhanden sind.

- console.aws.amazon.com
- signin.aws.amazon.com
- region.console.aws.amazon.com
- region.signin.aws.amazon.com
- support.console.aws.amazon.com

- global.console.aws.amazon.com
- Zusätzliche Datensätze in den zuvor aufgelisteten JSON-Dateien

VPC-Endpunkte und DNS Konfiguration für Dienste AWS

Die AWS Management Console Aufrufe erfolgen AWS-Services über eine Kombination aus direkten Browseranfragen und Anfragen, die von Webservern weitergeleitet werden. Um diesen Datenverkehr an Ihren AWS Management Console VPC-Endpunkt weiterzuleiten, müssen Sie den VPC-Endpunkt hinzufügen und DNS für jeden abhängigen AWS Dienst konfigurieren.

In den folgenden json Dateien sind die AWS PrivateLink unterstützten Dateien aufgeführt AWS-Services , die Sie verwenden können. Wenn ein Dienst nicht in diese Dateien integriert ist AWS PrivateLink, ist er nicht in diesen Dateien enthalten.

- https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
- https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
- https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json
- https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/il-central-1.config.json

Verwenden Sie das `ServiceName`-Feld für den VPC-Endpunkt des entsprechenden Services, um ihn zu Ihrer VPC hinzuzufügen.

> **Note**
>
> Wir aktualisieren diese Liste jeden Monat, da wir mehr Servicekonsolen um Unterstützung für AWS Management Console Private Access erweitern. Um auf dem neuesten Stand zu

bleiben, rufen Sie regelmäßig die vorherige Dateiliste ab und aktualisieren Sie Ihre VPC-Endpunkte.

Implementieren von Service-Kontrollrichtlinien und von VPC-Endpunktrichtlinien

Sie können Service Control Policies (SCPs) und VPC-Endpunktrichtlinien für AWS Management Console Private Access verwenden, um die Anzahl der Konten einzuschränken, die innerhalb Ihrer VPC und der AWS Management Console damit verbundenen lokalen Netzwerke verwendet werden dürfen.

AWS Management Console Private Access mit Dienststeuerungsrichtlinien verwenden AWS Organizations

Wenn Ihre AWS Organisation eine Service Control Policy (SCP) verwendet, die bestimmte Dienste zulässt, müssen Sie `signin:*` zu den zulässigen Aktionen weitere hinzufügen. Diese Berechtigung ist erforderlich, da bei der AWS Management Console Anmeldung am VPC-Endpunkt mit privatem Zugriff eine IAM-Autorisierung durchgeführt wird, die der SCP ohne die Erlaubnis blockiert. Beispielsweise ermöglicht die folgende Service-Kontrollrichtlinie die Nutzung von Amazon EC2 und CloudWatch Services in der Organisation, auch wenn auf sie über einen AWS Management Console Private Access-Endpunkt zugegriffen wird.

```
{
  "Effect": "Allow",
  "Action": [
    "signin:*",
    "ec2:*",
    "cloudwatch:*",
    ... Other services allowed
  },
  "Resource": "*"
}
```

Weitere Informationen zu SCPs finden Sie unter Service-Kontrollrichtlinien (SCPs) im AWS Organizations -Benutzerhandbuch.

Erlaube die AWS Management Console Nutzung nur für erwartete Konten und Organisationen (vertrauenswürdige Identitäten)

AWS Management Console und AWS-Anmeldung unterstützen eine VPC-Endpunktrichtlinie, die speziell die Identität des angemeldeten Kontos kontrolliert.

Im Gegensatz zu anderen VPC-Endpunktrichtlinien wird die Richtlinie vor der Authentifizierung evaluiert. Aus diesem Grund werden ausschließlich die Anmeldung und Nutzung der authentifizierten Sitzung und nicht die AWS dienstspezifischen Aktionen, die während der Sitzung ausgeführt werden, gesteuert. Wenn die Sitzung beispielsweise auf eine AWS Servicekonsole zugreift, z. B. die Amazon EC2 EC2-Konsole, werden diese VPC-Endpunktrichtlinien nicht anhand der Amazon EC2 EC2-Aktionen bewertet, die zur Anzeige dieser Seite ergriffen werden. Stattdessen können Sie die IAM-Richtlinien verwenden, die dem angemeldeten IAM-Principal zugeordnet sind, um dessen Genehmigung für Serviceaktionen zu kontrollieren. AWS

> **Note**
>
> VPC-Endpunktrichtlinien für AWS Management Console und SignIn VPC-Endpunkte unterstützen nur einen begrenzten Teil der Richtlinienformulierungen. Jeder `Principal` und jede `Resource` sollte auf * festgelegt sein und die `Action` sollte entweder * oder `signin:*` sein. Sie steuern den Zugriff auf VPC-Endpunkte mithilfe von `aws:PrincipalOrgId`- und `aws:PrincipalAccount`-Bedingungsschlüsseln.

Die folgenden Richtlinien werden sowohl für die Konsole als auch für die SignIn VPC-Endpoints empfohlen.

Diese VPC-Endpunktrichtlinie ermöglicht die Anmeldung AWS-Konten bei der angegebenen AWS Organisation und blockiert die Anmeldung bei allen anderen Konten.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
```

```
        "StringEquals": {
          "aws:PrincipalOrgId": "o-xxxxxxxxxxx"
        }
      }
    }
  ]
}
```

Diese VPC-Endpunktrichtlinie beschränkt die Anmeldung auf eine bestimmte Liste AWS-Konten und blockiert die Anmeldung bei allen anderen Konten.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": [ "111122223333", "222233334444" ]
        }
      }
    }
  ]
}
```

Richtlinien, die eine Organisation auf den VPC-Endpunkten AWS Management Console und Sign-In einschränken AWS-Konten , werden zum Zeitpunkt der Anmeldung bewertet und in regelmäßigen Abständen für bestehende Sitzungen neu bewertet.

Implementierung identitätsbasierter Richtlinien und anderer Richtlinientypen

Sie verwalten den Zugriff, AWS indem Sie Richtlinien erstellen und diese an IAM-Identitäten (Benutzer, Benutzergruppen oder Rollen) oder Ressourcen anhängen. AWS Auf dieser Seite wird beschrieben, wie Richtlinien funktionieren, wenn sie zusammen mit AWS Management Console Private Access verwendet werden.

Unterstützte Kontextschlüssel für AWS globale Bedingungen

AWS Management Console Private Access unterstützt `aws:SourceVpce` keine `aws:VpcSourceIp` AWS globalen Bedingungskontextschlüssel. Sie können stattdessen die `aws:SourceVpc`-IAM-Bedingung in Ihren Richtlinien verwenden, wenn Sie AWS Management Console Private Access verwenden.

So funktioniert AWS Management Console Private Access mit aws: SourceVpc

In diesem Abschnitt werden die verschiedenen Netzwerkpfade beschrieben, über die die von Ihnen generierten Anfragen weitergeleitet AWS Management Console werden können AWS-Services. Im Allgemeinen werden AWS Servicekonsolen mit einer Mischung aus direkten Browseranfragen und Anfragen implementiert, an die die AWS Management Console Webserver weiterleiten. AWS-Services Diese Implementierungen können ohne vorherige Ankündigung geändert werden. Wenn Ihre Sicherheitsanforderungen den Zugriff AWS-Services auf VPC-Endpunkte beinhalten, empfehlen wir Ihnen, VPC-Endpunkte für alle Dienste zu konfigurieren, die Sie von VPC aus verwenden möchten, sei es direkt oder über Private Access. AWS Management Console Darüber hinaus müssen Sie in Ihren Richtlinien die `aws:SourceVpc` IAM-Bedingung verwenden und nicht bestimmte `aws:SourceVpce` Werte für die Private Access-Funktion. AWS Management Console Dieser Abschnitt enthält Einzelheiten zur Funktionsweise der verschiedenen Netzwerkpfade.

Nachdem sich ein Benutzer bei angemeldet hat AWS Management Console, stellt er Anfragen AWS-Services über eine Kombination aus direkten Browseranfragen und Anfragen, die von AWS Management Console Webservern an Server weitergeleitet werden. AWS Anfragen zu CloudWatch Grafikdaten werden beispielsweise direkt vom Browser aus gestellt. Einige Anfragen an die AWS Servicekonsole, wie Amazon S3, werden dagegen vom Webserver per Proxy an Amazon S3 weitergeleitet.

Bei direkten Browseranfragen ändert die Verwendung von AWS Management Console Private Access nichts. Wie zuvor erreicht die Anfrage den Services über den Netzwerkpfad, den die VPC für monitoring.region.amazonaws.com konfiguriert hat. Wenn die VPC mit einem VPC-Endpunkt für konfiguriert istcom.amazonaws.region.monitoring, wird die Anfrage CloudWatch über diesen CloudWatch VPC-Endpunkt erreicht. Wenn es keinen VPC-Endpunkt für gibt CloudWatch, erreicht CloudWatch die Anfrage ihren öffentlichen Endpunkt über ein Internet Gateway auf der VPC. Anfragen, die über den CloudWatch VPC-Endpunkt CloudWatch eingehen, haben die IAM-Bedingungen `aws:SourceVpc` und werden auf ihre jeweiligen Werte `aws:SourceVpce` gesetzt. Diejenigen, die CloudWatch den öffentlichen Endpunkt erreichen, werden auf die Quell-IP-Adresse

der Anfrage `aws:SourceIp` eingestellt. Weitere Informationen über diese IAM-Bedingungsschlüssel finden Sie unter Globale Bedingungsschlüssel im IAM-Benutzerhandbuch.

Für Anfragen, die vom AWS Management Console Webserver weitergeleitet werden, wie z. B. die Anfrage, die die Amazon S3 S3-Konsole stellt, um Ihre Buckets aufzulisten, wenn Sie die Amazon S3 S3-Konsole aufrufen, ist der Netzwerkpfad anders. Diese Anfragen werden nicht von Ihrer VPC initiiert und verwenden daher nicht den VPC-Endpunkt, den Sie möglicherweise auf Ihrer VPC für diesen Service konfiguriert haben. Selbst wenn Sie in diesem Fall einen VPC-Endpunkt für Amazon S3 haben, verwendet die Anforderung Ihrer Sitzung an Amazon S3, die Buckets aufzulisten, nicht den Amazon S3-VPC-Endpunkt. Wenn Sie AWS Management Console Private Access jedoch mit unterstützten Diensten verwenden, enthalten diese Anfragen (z. B. an Amazon S3) den `aws:SourceVpc` Bedingungsschlüssel in ihrem Anforderungskontext. Der `aws:SourceVpc` Bedingungsschlüssel wird auf die VPC-ID gesetzt, auf der Ihre AWS Management Console Private Access-Endpunkte für die Anmeldung und die Konsole bereitgestellt werden. Wenn Sie also `aws:SourceVpc`-Einschränkungen in Ihren identitätsbasierten Richtlinien verwenden, müssen Sie die VPC-ID dieser VPC hinzufügen, die die AWS Management Console Private Access-SignIn- und Konsolenendpunkte hostet. Die `aws:SourceVpce`-Bedingung wird auf die jeweiligen SignIn- oder Konsolen-VPC-Endpunkt-IDs gesetzt.

> **Note**
>
> Wenn Ihre Benutzer Zugriff auf Servicekonsolen benötigen, die nicht von AWS Management Console Private Access unterstützt werden, müssen Sie eine Liste Ihrer erwarteten öffentlichen Netzwerkadressen (z. B. Ihren On-Premises-Netzwerkbereich) hinzufügen, indem Sie den `aws:SourceIP`-Bedingungsschlüssel in den identitätsbasierten Richtlinien der Benutzer verwenden.

Wie sich unterschiedliche Netzwerkpfade widerspiegeln in CloudTrail

Verschiedene Netzwerkpfade, die von Ihnen generierten Anfragen verwendet wurden, AWS Management Console spiegeln sich in Ihrem CloudTrail Eventverlauf wider.

Bei direkten Browseranfragen ändert die Verwendung von AWS Management Console Private Access nichts. CloudTrail Ereignisse enthalten Details zur Verbindung, z. B. die VPC-Endpunkt-ID, die für den API-Aufruf des Dienstes verwendet wurde.

Bei Anfragen, die vom AWS Management Console Webserver als Proxy weitergeleitet werden, enthalten die CloudTrail Ereignisse keine VPC-bezogenen Details. Erste Anfragen, AWS-Anmeldung

die für die Einrichtung der Browsersitzung erforderlich sind, wie z. B. der `AwsConsoleSignIn` Ereignistyp, enthalten jedoch die AWS-Anmeldung VPC-Endpunkt-ID in den Ereignisdetails.

Versuchen Sie es AWS Management Console mit Private Access

In diesem Abschnitt wird beschrieben, wie Sie AWS Management Console Private Access in einem neuen Konto einrichten und testen.

AWS Management Console Private Access ist eine erweiterte Sicherheitsfunktion und erfordert Vorkenntnisse über Netzwerke und die Einrichtung von VPCs. In diesem Thema wird beschrieben, wie Sie AWS Management Console Private Access ohne eine umfassende Infrastruktur ausprobieren können.

Themen

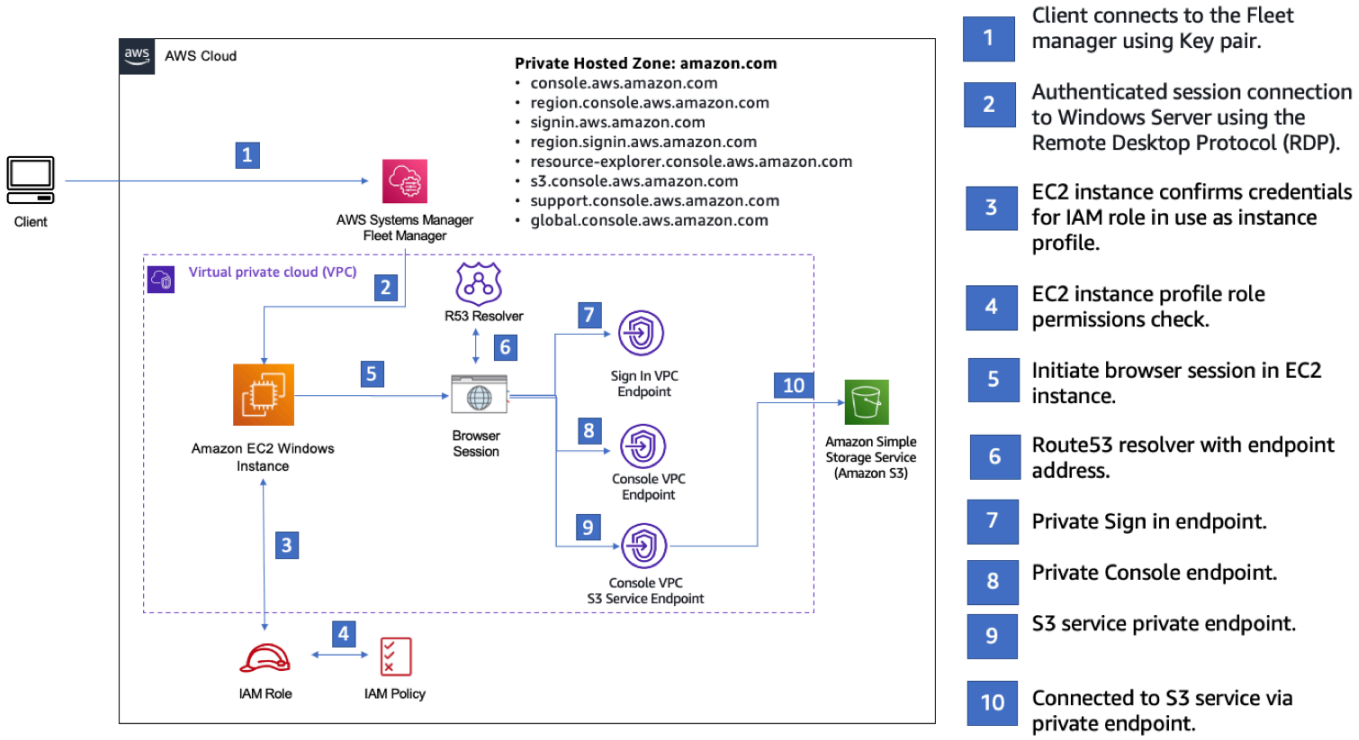
- Test-Setup mit Amazon EC2
- Test-Setup mit Amazon WorkSpaces
- Testen des VPC-Setups mit IAM-Richtlinien

Test-Setup mit Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der Amazon Web Services Cloud. Mit Amazon EC2 können Sie so viele oder so wenige virtuelle Server starten, wie Sie benötigen, die Sicherheit und das Netzwerk konfigurieren und den Speicher verwalten. Bei dieser Einrichtung verwenden wir Fleet Manager, eine Funktion von AWS Systems Manager, um eine Verbindung zu Ihrer Amazon EC2 Windows Instance mithilfe des Remote Desktop Protocol (RDP) herzustellen.

Dieses Handbuch zeigt eine Testumgebung, um eine AWS Management Console Private Access-Verbindung zu Amazon Simple Storage Service von einer Amazon EC2 EC2-Instance aus einzurichten und zu nutzen. In diesem Tutorial wird AWS CloudFormation das Netzwerk-Setup erstellt und konfiguriert, das von Amazon EC2 zur Visualisierung dieser Funktion verwendet werden soll.

Das folgende Diagramm beschreibt den Vorgang für die Verwendung von Amazon EC2 für den Zugriff auf ein AWS Management Console Private Access-Setup. Es zeigt, wie ein Benutzer über einen privaten Endpunkt mit Amazon S3 verbunden wird.



Kopieren Sie die folgende AWS CloudFormation Vorlage und speichern Sie sie in einer Datei, die Sie in Schritt drei des Verfahrens So richten Sie ein Netzwerk ein.

> **Note**
>
> Diese AWS CloudFormation Vorlage verwendet Konfigurationen, die derzeit in der Region Israel (Tel Aviv) nicht unterstützt werden.

AWS Management Console Amazon EC2 AWS CloudFormation EC2-Vorlage für private Zugriffsumgebung

```
Description: |
  AWS Management Console Private Access.
Parameters:
  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
    Description: CIDR range for VPC
```

```
  Ec2KeyPair:
    Type: AWS::EC2::KeyPair::KeyName
    Description: The EC2 KeyPair to use to connect to the Windows instance

  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
    Description: CIDR range for Public Subnet A

  PublicSubnet2CIDR:
    Type: String
    Default: 172.16.0.0/24
    Description: CIDR range for Public Subnet B

  PublicSubnet3CIDR:
    Type: String
    Default: 172.16.2.0/24
    Description: CIDR range for Public Subnet C

  PrivateSubnet1CIDR:
    Type: String
    Default: 172.16.4.0/24
    Description: CIDR range for Private Subnet A

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
    Description: CIDR range for Private Subnet B

  PrivateSubnet3CIDR:
    Type: String
    Default: 172.16.3.0/24
    Description: CIDR range for Private Subnet C

  LatestWindowsAmiId:
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
    Default: '/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base'

  InstanceTypeParameter:
    Type: String
    Default: 't2.medium'


Resources:
```

```
#########################
# VPC AND SUBNETS
#########################

  AppVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: !Ref VpcCIDR
      InstanceTenancy: default
      EnableDnsSupport: true
      EnableDnsHostnames: true

  PublicSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet1CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 0
          - Fn::GetAZs: ""

  PublicSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet2CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 1
          - Fn::GetAZs: ""

  PublicSubnetC:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet3CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 2
```

```
        - Fn::GetAZs: ""

  PrivateSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
      AvailabilityZone:
        Fn::Select:
          - 0
          - Fn::GetAZs: ""

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone:
        Fn::Select:
          - 1
          - Fn::GetAZs: ""

  PrivateSubnetC:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet3CIDR
      AvailabilityZone:
        Fn::Select:
          - 2
          - Fn::GetAZs: ""

  InternetGateway:
    Type: AWS::EC2::InternetGateway

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment
```

```
  NatGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

########################
# Route Tables
########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway

  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetA

  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB

  PrivateSubnetRouteTableAssociation3:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetC

  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
```

```
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB

  PublicSubnetBRouteTableAssociation3:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetC


##########################
# SECURITY GROUPS
##########################

  VPCEndpointSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
          CidrIp: !GetAtt AppVPC.CidrBlock
```

```
  EC2SecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Default EC2 Instance SG
      VpcId: !Ref AppVPC

#########################
# VPC ENDPOINTS
#########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSSM:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssm'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceEc2messages:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ec2messages'
```

```
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceSsmmessages:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssmmessages'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceConsole:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
      VpcId: !Ref AppVPC
```

```
#########################
# ROUTE53 RESOURCES
#########################

  ConsoleHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  ConsoleRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  GlobalConsoleRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'global.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleS3ProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 's3.console.aws.amazon.com'
```

```
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleSupportProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "support.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ExplorerProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "resource-explorer.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  SigninHostedZone:
```

```
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  SigninRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

  SigninRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

#########################
# EC2 INSTANCE
#########################

  Ec2InstanceRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
```

```
        -
          Effect: Allow
          Principal:
            Service:
              - ec2.amazonaws.com
          Action:
            - sts:AssumeRole
    Path: /
    ManagedPolicyArns:
      - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

Ec2InstanceProfile:
  Type: AWS::IAM::InstanceProfile
  Properties:
    Path: /
    Roles:
     - !Ref Ec2InstanceRole

EC2WinInstance:
  Type: 'AWS::EC2::Instance'
  Properties:
    ImageId: !Ref LatestWindowsAmiId
    IamInstanceProfile: !Ref Ec2InstanceProfile
    KeyName: !Ref Ec2KeyPair
    InstanceType:
      Ref: InstanceTypeParameter
    SubnetId: !Ref PrivateSubnetA
    SecurityGroupIds:
      - Ref: EC2SecurityGroup
    BlockDeviceMappings:
      - DeviceName: /dev/sda1
        Ebs:
          VolumeSize: 50
    Tags:
    - Key: "Name"
      Value: "Console VPCE test instance"
```

So richten Sie ein Netzwerk ein:

1. Melden Sie sich bei dem Verwaltungskonto Ihrer Organisation an, und öffnen Sie die AWS CloudFormation -Konsole.
2. Wählen Sie Stack erstellen aus.

3. Wählen Sie Mit neuen Ressourcen (Standard). Laden Sie die AWS CloudFormation Vorlagendatei hoch, die Sie zuvor erstellt haben, und wählen Sie Weiter.
4. Geben Sie einen Namen für den Stack ein, z. B. **`PrivateConsoleNetworkForS3`**, und wählen Sie Weiter aus.
5. Geben Sie für VPC und Subnetze Ihre bevorzugten IP-CIDR-Bereiche ein, oder verwenden Sie die angegebenen Standardwerte. Wenn Sie die Standardwerte verwenden, stellen Sie sicher, dass sie sich nicht mit den vorhandenen VPC-Ressourcen in Ihrem AWS-Kontoüberschneiden.
6. Wählen Sie für den KeyPairEc2-Parameter eines der vorhandenen Amazon EC2 EC2-Schlüsselpaare in Ihrem Konto aus. Wenn Sie nicht über ein vorhandenes Amazon EC2-Schlüsselpaar verfügen, müssen Sie eines erstellen, bevor Sie mit dem nächsten Schritt fortfahren. Weitere Informationen finden Sie unter Erstellen eines key pair mit Amazon EC2 im Amazon EC2 EC2-Benutzerhandbuch.
7. Wählen Sie Stack erstellen aus.
8. Nachdem der Stack erstellt wurde, wählen Sie die Registerkarte Ressourcen, um die erstellten Ressourcen anzuzeigen.

So stellen Sie eine Verbindung zu Ihrer Amazon-EC2-Instance her:

1. Melden Sie sich bei dem Verwaltungskonto für Ihre Organisation an, und öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie auf der Seite Instances die VPCE-Testinstanz für die Konsole aus, die mit der Vorlage erstellt wurde. AWS CloudFormation Wählen Sie dann Verbinden aus.

> **Note**
>
> In diesem Beispiel wird Fleet Manager, eine Funktion von AWS Systems Manager Explorer, verwendet, um eine Verbindung zu Ihrem Windows Server herzustellen. Es kann einige Minuten dauern, bis die Verbindung hergestellt werden kann.

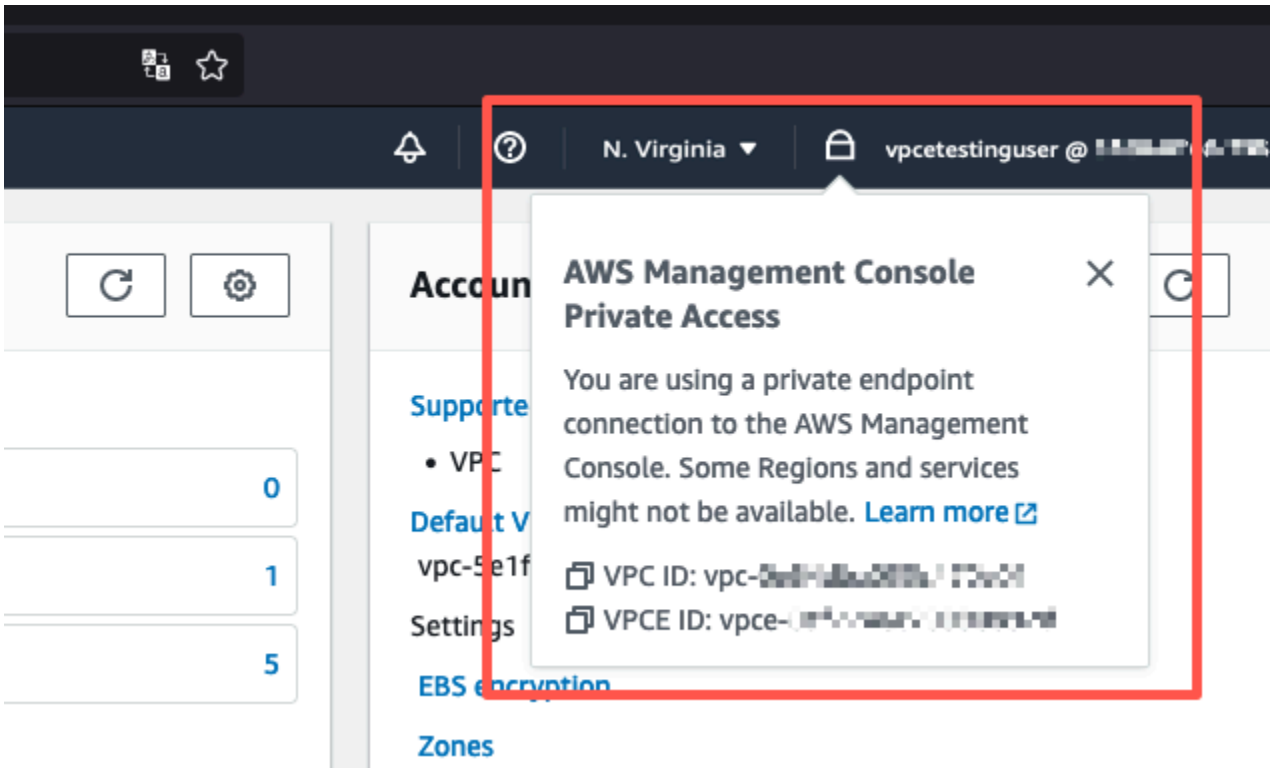
4. Wählen Sie auf der Seite Mit Instance verbinden die Option RDP Client und dann Mit Fleet Manager verbinden aus.
5. Wählen Sie Fleet Manager Remote Destop aus.
6. Um das Administratorkennwort für die Amazon EC2 EC2-Instance abzurufen und über die Weboberfläche auf den Windows-Desktop zuzugreifen, verwenden Sie den privaten Schlüssel,

der dem Amazon EC2 EC2-Schlüsselpaar zugeordnet ist, das Sie bei der Erstellung der AWS CloudFormation Vorlage verwendet haben.

7. Öffnen Sie von der Amazon EC2 EC2-Windows-Instance aus die AWS Management Console im Browser.
8. Nachdem Sie sich mit Ihren AWS Anmeldeinformationen angemeldet haben, öffnen Sie die Amazon S3 S3-Konsole und stellen Sie sicher, dass Sie über AWS Management Console Private Access verbunden sind.

Um die Einrichtung von AWS Management Console Private Access zu testen

1. Melden Sie sich beim Verwaltungskonto Ihrer Organisation an, und öffnen Sie die Amazon S3-Konsole.
2. Wählen Sie das Lock-Private-Symbol in der Navigationsleiste, um den VPC-Endpunkt anzuzeigen. Der folgende Screenshot zeigt die Position des Lock-Private-Symbols und der VPC-Informationen.



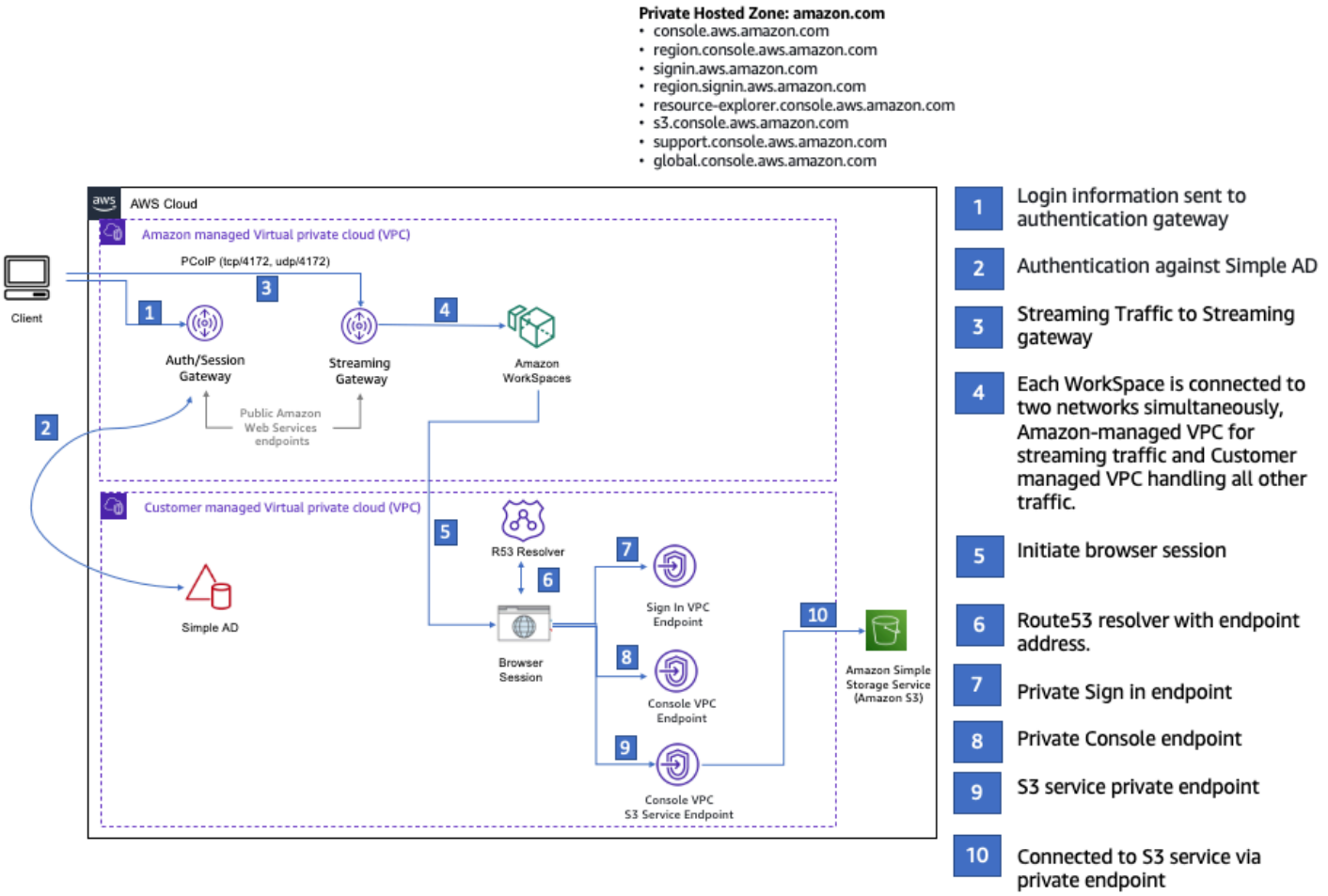
Test-Setup mit Amazon WorkSpaces

Amazon WorkSpaces ermöglicht Ihnen die Bereitstellung virtueller, Cloud-basierter Windows-, Amazon Linux- oder Ubuntu-Linux-Desktops für Ihre Benutzer, bekannt als WorkSpaces. Sie können nach Ihren Bedürfnissen Benutzer schnell und bequem hinzufügen oder entfernen. Benutzer können auf ihre virtuellen Desktops von mehreren Geräten oder Web-Browsern aus zugreifen. Weitere Informationen WorkSpaces dazu finden Sie im Amazon WorkSpaces Administration Guide.

Das Beispiel in diesem Abschnitt beschreibt eine Testumgebung, in der eine Benutzerumgebung einen Webbrowser verwendet, der auf einem läuft WorkSpace , um sich bei AWS Management Console Private Access anzumelden. Anschließend besucht der Benutzer die Amazon Simple Storage Service-Konsole. Dies WorkSpace soll die Erfahrung eines Unternehmensbenutzers mit einem Laptop in einem mit VPN verbundenen Netzwerk simulieren, der AWS Management Console über seinen Browser darauf zugreift.

In diesem Tutorial werden das Netzwerk-Setup und ein Simple Active Directory erstellt und konfiguriert, das verwendet werden soll, WorkSpaces sowie eine schrittweise Anleitung zur Einrichtung eines WorkSpace mit dem. AWS CloudFormation AWS Management Console

Das folgende Diagramm beschreibt den Arbeitsablauf für die Verwendung von a WorkSpace zum Testen eines AWS Management Console privaten Zugriffssetups. Es zeigt die Beziehung zwischen einem Kunden WorkSpace, einer von Amazon verwalteten VPC und einer vom Kunden verwalteten VPC.



Kopieren Sie die folgende AWS CloudFormation Vorlage und speichern Sie sie in einer Datei, die Sie in Schritt 3 des Verfahrens zum Einrichten eines Netzwerks verwenden werden.

AWS Management ConsoleAWS CloudFormation Vorlage für eine private Zugriffsumgebung

```
Description: |
  AWS Management Console Private Access.
Parameters:

  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
    Description: CIDR range for VPC

  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
```

```
    Description: CIDR range for Public Subnet A

  PublicSubnet2CIDR:
    Type: String
    Default: 172.16.0.0/24
    Description: CIDR range for Public Subnet B

  PrivateSubnet1CIDR:
    Type: String
    Default: 172.16.4.0/24
    Description: CIDR range for Private Subnet A

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
    Description: CIDR range for Private Subnet B

# Amazon WorkSpaces is available in a subset of the Availability Zones for each
 supported Region.
# https://docs.aws.amazon.com/workspaces/latest/adminguide/azs-workspaces.html
Mappings:
  RegionMap:
    us-east-1:
      az1: use1-az2
      az2: use1-az4
      az3: use1-az6
    us-west-2:
      az1: usw2-az1
      az2: usw2-az2
      az3: usw2-az3
    ap-south-1:
      az1: aps1-az1
      az2: aps1-az2
      az3: aps1-az3
    ap-northeast-2:
      az1: apne2-az1
      az2: apne2-az3
    ap-southeast-1:
      az1: apse1-az1
      az2: apse1-az2
    ap-southeast-2:
      az1: apse2-az1
      az2: apse2-az3
    ap-northeast-1:
```

```
      az1: apne1-az1
      az2: apne1-az4
    ca-central-1:
      az1: cac1-az1
      az2: cac1-az2
    eu-central-1:
      az1: euc1-az2
      az2: euc1-az3
    eu-west-1:
      az1: euw1-az1
      az2: euw1-az2
    eu-west-2:
      az1: euw2-az2
      az2: euw2-az3
    sa-east-1:
      az1: sae1-az1
      az2: sae1-az3

Resources:

  iamLambdaExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
              - lambda.amazonaws.com
            Action:
              - 'sts:AssumeRole'
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
      Policies:
        - PolicyName: describe-ec2-az
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
              - Effect: Allow
                Action:
                  - 'ec2:DescribeAvailabilityZones'
                Resource: '*'
      MaxSessionDuration: 3600
```

```
      Path: /service-role/

  fnZoneIdtoZoneName:
    Type: AWS::Lambda::Function
    Properties:
      Runtime: python3.8
      Handler: index.lambda_handler
      Code:
        ZipFile: |
          import boto3
          import cfnresponse

          def zoneId_to_zoneName(event, context):
              responseData = {}
              ec2 = boto3.client('ec2')
              describe_az = ec2.describe_availability_zones()
              for az in describe_az['AvailabilityZones']:
                  if event['ResourceProperties']['ZoneId'] == az['ZoneId']:
                      responseData['ZoneName'] = az['ZoneName']
                      cfnresponse.send(event, context, cfnresponse.SUCCESS,
responseData, str(az['ZoneId']))

          def no_op(event, context):
              print(event)
              responseData = {}
              cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
str(event['RequestId']))

          def lambda_handler(event, context):
              if event['RequestType'] == ('Create' or 'Update'):
                  zoneId_to_zoneName(event, context)
              else:
                  no_op(event,context)
      Role: !GetAtt iamLambdaExecutionRole.Arn

  getAZ1:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az1 ]
  getAZ2:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
```

```
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az2 ]

########################
# VPC AND SUBNETS
########################

  AppVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: !Ref VpcCIDR
      InstanceTenancy: default
      EnableDnsSupport: true
      EnableDnsHostnames: true

  PublicSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet1CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PublicSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet2CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ2.ZoneName

  PrivateSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone: !GetAtt getAZ2.ZoneName
```

```
  InternetGateway:
    Type: AWS::EC2::InternetGateway

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment

  NatGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

#########################
# Route Tables
#########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway

  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetA

  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
```

```
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB

  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB


##########################
# SECURITY GROUPS
##########################

  VPCEndpointSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
          CidrIp: !GetAtt AppVPC.CidrBlock
```

```
##########################
# VPC ENDPOINTS
##########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceConsole:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
      VpcId: !Ref AppVPC

##########################
# ROUTE53 RESOURCES
##########################

  ConsoleHostedZone:
```

```
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  ConsoleRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  GlobalConsoleRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'global.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleS3ProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 's3.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
      Type: A

  ConsoleSupportProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "support.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ExplorerProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "resource-explorer.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  SigninHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
```

```
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  SigninRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

  SigninRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

#########################
# WORKSPACE RESOURCES
#########################
  ADAdminSecret:
    Type: AWS::SecretsManager::Secret
    Properties:
      Name: "ADAdminSecret"
      Description: "Password for directory services admin"
      GenerateSecretString:
        SecretStringTemplate: '{"username": "Admin"}'
        GenerateStringKey: password
        PasswordLength: 30
        ExcludeCharacters: '"@/\'

  WorkspaceSimpleDirectory:
```

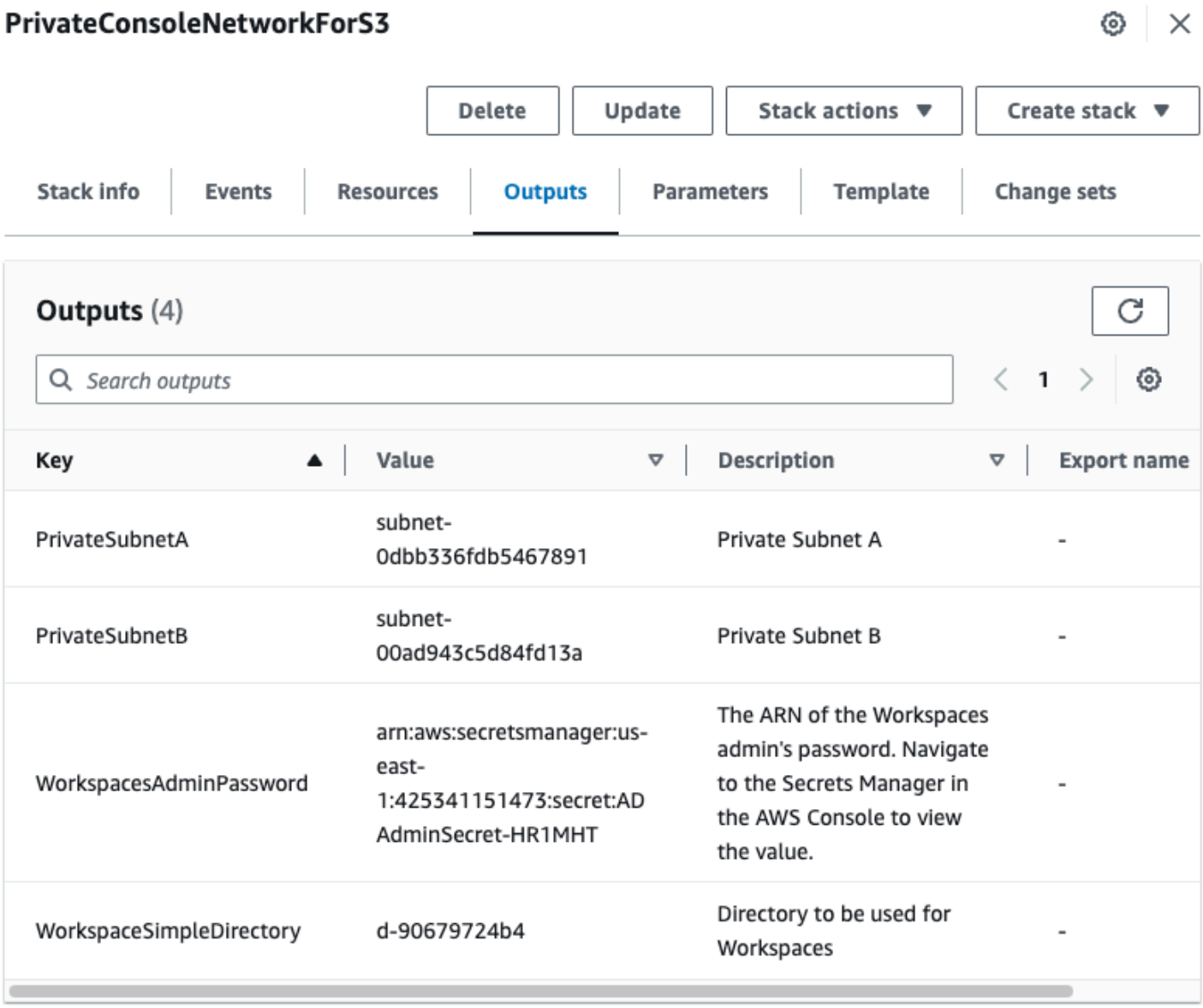
```
    Type: AWS::DirectoryService::SimpleAD
    DependsOn: AppVPC
    DependsOn: PrivateSubnetA
    DependsOn: PrivateSubnetB
    Properties:
      Name: "corp.awsconsole.com"
      Password: '{{resolve:secretsmanager:ADAdminSecret:SecretString:password}}'
      Size: "Small"
      VpcSettings:
        SubnetIds:
          - Ref: PrivateSubnetA
          - Ref: PrivateSubnetB

        VpcId:
          Ref: AppVPC


Outputs:
  PrivateSubnetA:
    Description: Private Subnet A
    Value: !Ref PrivateSubnetA

  PrivateSubnetB:
    Description: Private Subnet B
    Value: !Ref PrivateSubnetB

  WorkspaceSimpleDirectory:
    Description: Directory to be used for Workspaces
    Value: !Ref WorkspaceSimpleDirectory

  WorkspacesAdminPassword:
    Description : "The ARN of the Workspaces admin's password.  Navigate to the Secrets
 Manager in the AWS Console to view the value."
    Value: !Ref ADAdminSecret
```

> **Note**
>
> Dieses Test-Setup ist für den Betrieb in der Region USA Ost (Nord-Virginia) (us-east-1) konzipiert.

So richten Sie ein Netzwerk ein:

1. Melden Sie sich bei dem Verwaltungskonto Ihrer Organisation an, und öffnen Sie die AWS CloudFormation -Konsole.
2. Wählen Sie Stack erstellen aus.
3. Wählen Sie Mit neuen Ressourcen (Standard). Laden Sie die AWS CloudFormation Vorlagendatei hoch, die Sie zuvor erstellt haben, und wählen Sie Weiter.
4. Geben Sie einen Namen für den Stack ein, z. B. **`PrivateConsoleNetworkForS3`**, und wählen Sie Weiter aus.
5. Geben Sie für VPC und Subnetze Ihre bevorzugten IP-CIDR-Bereiche ein, oder verwenden Sie die angegebenen Standardwerte. Wenn Sie die Standardwerte verwenden, stellen Sie sicher, dass sie sich nicht mit den vorhandenen VPC-Ressourcen in Ihrem AWS-Kontoüberschneiden.
6. Wählen Sie Stack erstellen aus.
7. Nachdem der Stack erstellt wurde, wählen Sie die Registerkarte Ressourcen, um die erstellten Ressourcen anzuzeigen.
8. Wählen Sie die Registerkarte Ausgaben, um die Werte für private Subnetze und das Workspace Simple Directory anzuzeigen. Notieren Sie sich diese Werte, da Sie sie in Schritt 4 des nächsten Verfahrens zum Erstellen und Konfigurieren eines WorkSpace verwenden werden.

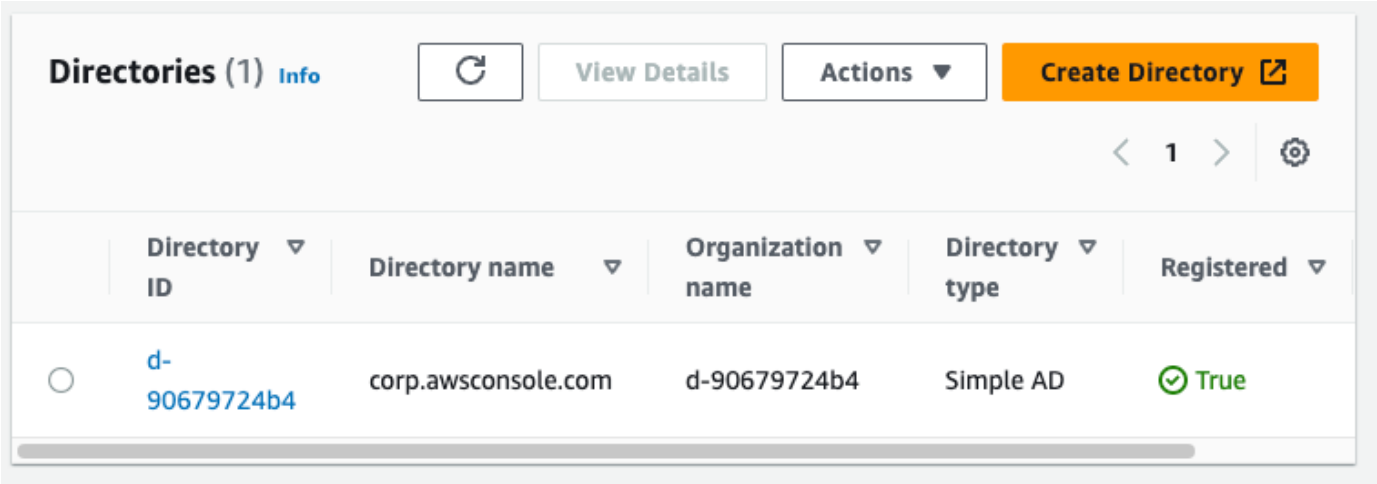
Der folgende Screenshot zeigt die Ansicht der Registerkarte Ausgaben, in der die Werte für die privaten Subnetze und das Workspace Simple Directory angezeigt werden.



Nachdem Sie Ihr Netzwerk erstellt haben, gehen Sie wie folgt vor, um ein Netzwerk zu erstellen und darauf zuzugreifen WorkSpace.

Um ein zu erstellen WorkSpace

1. Öffnen Sie die WorkSpaces -Konsole.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Vergewissern Sie sich auf der Seite Verzeichnisse, dass der Verzeichnisstatus Aktiv ist. Der folgende Screenshot zeigt eine Verzeichnisseite mit einem aktiven Verzeichnis.



4. Um ein Verzeichnis in verwenden zu können WorkSpaces, müssen Sie es registrieren. Wählen Sie im Navigationsbereich WorkSpacesund anschließend Erstellen aus WorkSpaces.
5. Wählen Sie unter Verzeichnis auswählen das Verzeichnis aus, das von AWS CloudFormation im vorherigen Verfahren erstellt wurde. Wählen Sie im Menü Aktionen die Option Registrieren.
6. Wählen Sie für die Subnetzauswahl die beiden privaten Subnetze aus, die in Schritt 9 des vorherigen Verfahrens beschrieben wurden.
7. Wählen Sie Self-Service-Berechtigungen aktivieren und anschließend Registrieren aus.
8. Nachdem das Verzeichnis registriert wurde, fahren Sie mit der Erstellung des fort WorkSpace. Wählen Sie das registrierte Verzeichnis aus, und wählen Sie dann Weiter.
9. Wählen Sie auf der Seite Benutzer erstellen die Option Zusätzlichen Benutzer erstellen aus. Geben Sie Ihren Namen und Ihre E-Mail-Adresse ein, damit Sie den verwenden können WorkSpace. Stellen Sie sicher, dass die E-Mail-Adresse gültig ist, da die WorkSpace Anmeldeinformationen an diese E-Mail-Adresse gesendet werden.
10. Wählen Sie Weiter.
11. Wählen Sie auf der Seite Benutzer identifizieren den Benutzer aus, den Sie in Schritt 9 erstellt haben, und klicken Sie dann auf Weiter.
12. Wählen Sie auf der Seite Paket auswählen die Option Standard mit Amazon Linux 2 und anschließend Weiter.
13. Verwenden Sie die Standardeinstellungen für den Ausführungsmodus und die Benutzeranpassung, und wählen Sie anschließend Workspace erstellen. Das WorkSpace beginnt im `Pending` Status und geht `Available` innerhalb von etwa 20 Minuten über.
14. Sobald der verfügbar WorkSpace ist, erhalten Sie an die E-Mail-Adresse, die Sie in Schritt 9 angegeben haben, eine E-Mail mit Anweisungen, wie Sie darauf zugreifen können.

Nachdem Sie sich bei Ihrem angemeldet haben WorkSpace, können Sie testen, ob Sie mit Ihrem AWS Management Console privaten Zugang darauf zugreifen.

Um auf eine zuzugreifen WorkSpace

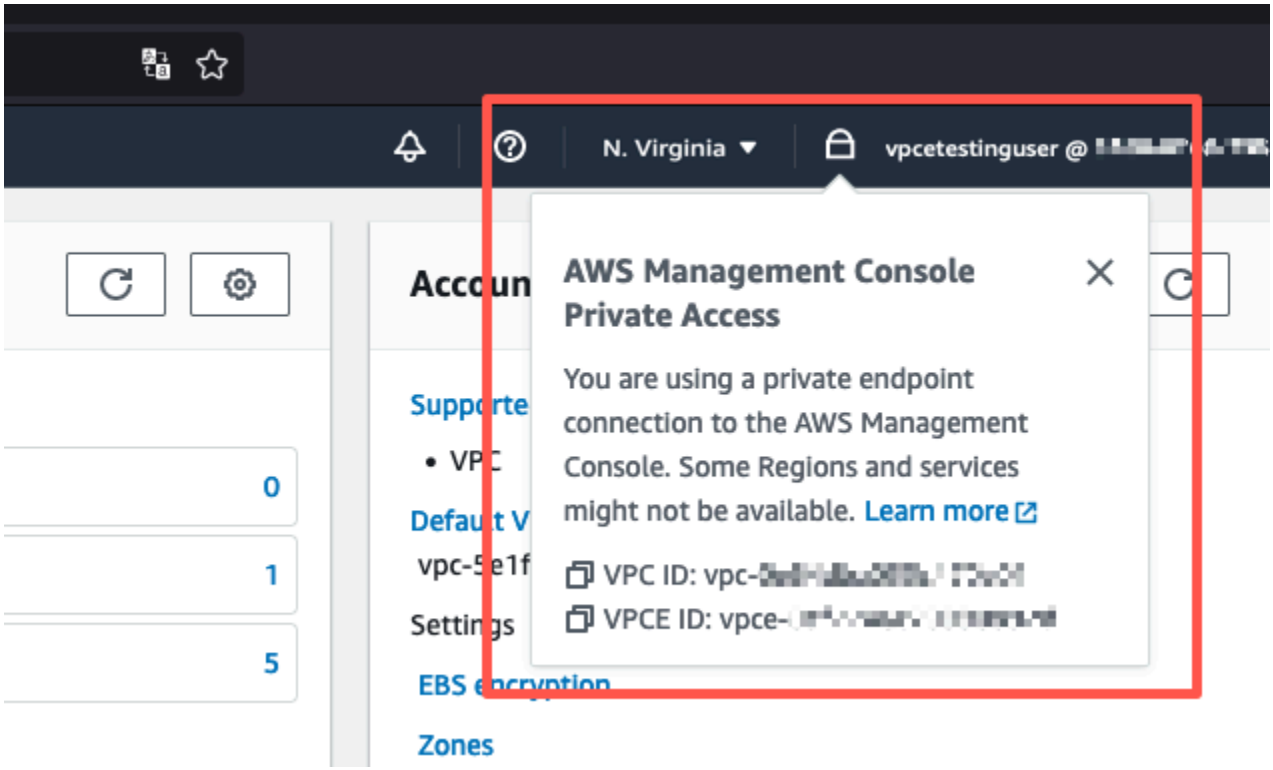
1. Öffnen Sie die E-Mail, die Sie in Schritt 14 des vorherigen Verfahrens erhalten haben.
2. Wählen Sie in der E-Mail den eindeutigen Link aus, mit dem Sie Ihr Profil einrichten und den WorkSpaces Client herunterladen können.
3. Richten Sie ihr Passwort ein.
4. Laden Sie den Client Ihrer Wahl herunter.
5. Installieren und starten Sie den Client. Geben Sie den Registrierungscode ein, der in Ihrer E-Mail angegeben wurde, und wählen Sie dann Registrieren.
6. Melden Sie sich WorkSpaces mit den Anmeldedaten, die Sie in Schritt 3 erstellt haben, bei Amazon an.

Um die Einrichtung von AWS Management Console Private Access zu testen

1. Öffnen Sie von Ihrem WorkSpace aus Ihren Browser. Navigieren Sie dann zur AWS Management Console und melden Sie sich mit Ihren Anmeldeinformationen an.

   > **Note**
   >
   > Wenn Sie Firefox als Browser verwenden, stellen Sie sicher, dass die Option DNS über HTTPS aktivieren in Ihren Browsereinstellungen deaktiviert ist.

2. Öffnen Sie die Amazon S3 S3-Konsole, in der Sie überprüfen können, ob Sie über AWS Management Console Private Access verbunden sind.
3. Wählen Sie das Lock-Private-Symbol in der Navigationsleiste, um die verwendete VPC und den VPC-Endpunkt anzuzeigen. Der folgende Screenshot zeigt die Position des Lock-Private-Symbols und der VPC-Informationen.



Testen des VPC-Setups mit IAM-Richtlinien

Sie können Ihre VPC, die Sie mit Amazon EC2 eingerichtet haben, weiter testen oder WorkSpaces indem Sie IAM-Richtlinien bereitstellen, die den Zugriff einschränken.

Die folgende Richtlinie verweigert den Zugriff auf Amazon S3, es sei denn, sie verwendet Ihre angegebene VPC.

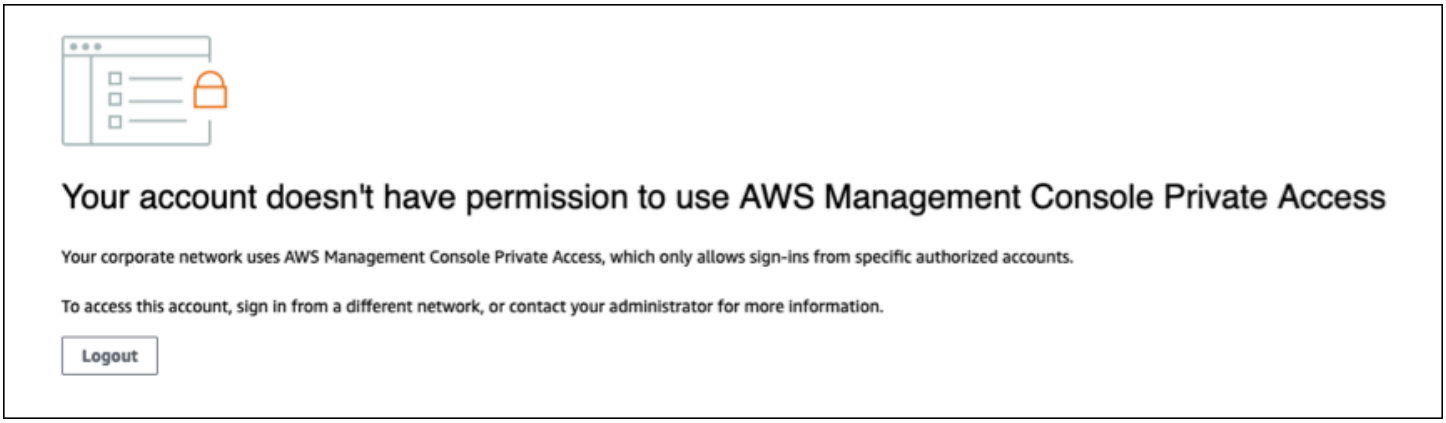
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "S3:*",
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": "sourceVPC"
                },
                "Bool": {
                    "aws:ViaAwsService": "false"
                }
```

```
            }
        }
    ]
}
```

Die folgende Richtlinie beschränkt die Anmeldung auf ausgewählte AWS-Konto IDs mithilfe einer AWS Management Console privaten Zugriffsrichtlinie für den Anmeldeendpunkt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "AWSAccountID"
                    ]
                }
            }
        }
    ]
}
```

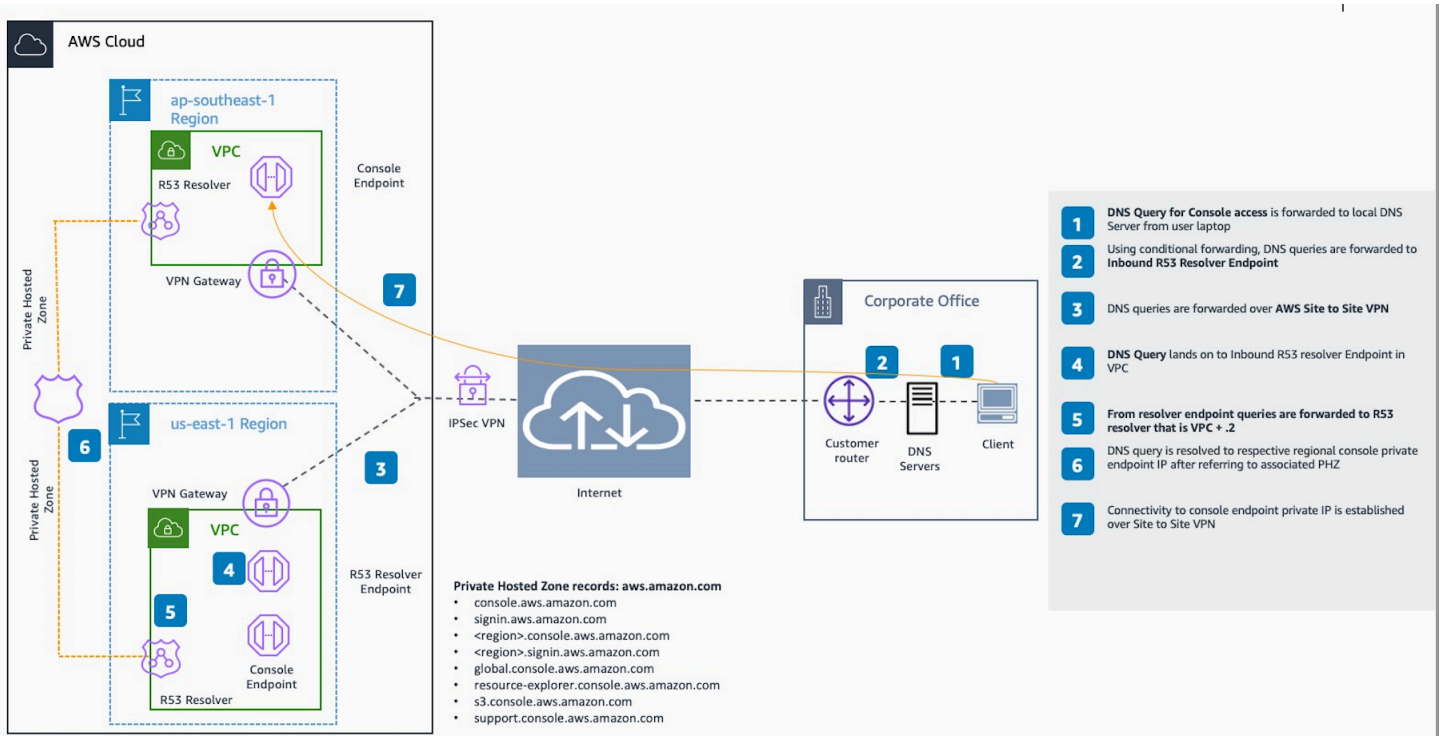
Wenn Sie eine Verbindung mit einer Identität herstellen, die nicht zu Ihrem Konto gehört, wird die folgende Fehlerseite angezeigt.



Referenzarchitektur

Um von einem lokalen Netzwerk aus eine AWS Management Console private Verbindung mit Private Access herzustellen, können Sie die Verbindungsoption AWS Site-to-Site VPN zu AWS Virtual Private Gateway (VGW) nutzen. AWS Site-to-Site VPN ermöglicht den Zugriff auf Ihr Remote-Netzwerk von Ihrer VPC aus, indem eine Verbindung hergestellt und das Routing so konfiguriert wird, dass der Datenverkehr über die Verbindung weitergeleitet wird. Weitere Informationen finden Sie unter Was ist AWS Site-to-Site VPN im Site-to-Site VPN AWS VPN-Benutzerhandbuch. AWS Virtual Private Gateway (VGW) ist ein hochverfügbarer regionaler Dienst, der als Gateway zwischen einer VPC und dem lokalen Netzwerk fungiert.

AWS Site-to-Site VPN zum AWS Virtual Private Gateway (VGW)



Ein wesentlicher Bestandteil dieses Referenzarchitekturentwurfs ist der Amazon Route 53 Resolver Inbound-Resolver. Wenn Sie es in der VPC einrichten, in der die AWS Management Console Private Access-Endpoints erstellt werden, werden Resolver-Endpunkte (Netzwerkschnittstellen) in den angegebenen Subnetzen erstellt. Ihre IP-Adressen können dann in bedingten Weiterleitungen auf den On-Premises DNS-Servern abgerufen werden, um die Abfrage von Datensätzen in einer privat gehosteten Zone zu ermöglichen. Wenn lokale Clients eine Verbindung zu herstellen AWS Management Console, werden sie an die privaten IP-Adressen der Private Access-Endpunkte weitergeleitet. AWS Management Console

Bevor Sie die Verbindung zum AWS Management Console Private Access-Endpunkt einrichten, müssen Sie die erforderlichen Schritte zur Einrichtung der AWS Management Console Private Access-Endpunkte in allen Regionen, auf die Sie zugreifen möchten AWS Management Console, sowie in der Region USA Ost (Nord-Virginia) abschließen und die Private Hosted Zone konfigurieren.

Starten von AWS CloudShell in der Konsolen-Symbolleiste

AWS CloudShell ist eine browserbasierte, vorab authentifizierte Shell, die Sie direkt über die AWS Management Console in der Konsolen-Symbolleiste starten können. Sie können AWS CLI-Befehle für Services ausführen, die Ihre bevorzugte Shell verwenden (Bash, PowerShell oder Z-Shell).

Sie können CloudShell auf eine der folgenden zwei Methoden in der Console Toolbar starten:

- Wählen Sie das CloudShell-Symbol unten links in der Konsole aus.
- Wählen Sie das CloudShell-Symbol in der oberen Navigationsleiste der Konsole aus.

Weitere Informationen zu diesem Service finden Sie im AWS CloudShell-Benutzerhandbuch.

Informationen über die AWS-Regionen, in denen AWS CloudShell verfügbar ist, finden Sie in der Liste der regionalen AWS-Services. Die Auswahl der Konsolenregion erfolgt synchron mit der CloudShell-Region. Wenn CloudShell in einer ausgewählten Region nicht verfügbar ist, wird CloudShell in der nächstgelegenen Region betrieben.

Abrufen von Rechnungsinformationen

Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie Informationen zu Ihren AWS-Gebühren über die Konsole abrufen.

So rufen Sie Ihre Rechnungsinformationen ab

1. Wählen Sie auf der Navigationsleiste den Namen Ihres Kontos aus.
2. Wählen Sie Billing Dashboard (Fakturierungs-Dashboard) aus.
3. Suchen Sie über das AWS Billing and Cost Management-Dashboard eine Zusammenfassung und eine Aufschlüsselung Ihrer monatlichen Ausgaben. Weitere Informationen finden Sie im AWS Billing-Benutzerhandbuch.

Verwenden von Markdown in der Konsole

Einige Dienste in der AWS Management Console, wie Amazon CloudWatch, unterstützen die Verwendung von Markdown in bestimmten Bereichen. In diesem Thema werden die in der Konsole unterstützten Typen der Markdown-Formatierung beschrieben.

Inhalt

Paragraphen, Zeilenabstand und horizontale Linien

Paragraphen werden durch eine Leerzeile getrennt. Um sicherzustellen, dass die Leerzeile zwischen den Paragraphen bei der Konvertierung in HTML gerendert wird, fügen Sie eine neue Zeile mit einem festen Leerzeichen (` `) und anschließend eine Leerzeile hinzu. Wenn Sie mehrere Leerzeilen nacheinander einfügen möchten, wiederholen Sie dies, wie im folgenden Beispiel gezeigt:

```
 

 
```

Zum Erstellen einer horizontalen Linie zur Trennung der Paragraphen fügen Sie eine neue Zeile mit drei Bindestrichen hintereinander ein: `---`

```
Previous paragraph.
---
Next paragraph.
```

Zum Erstellen eines Textblocks mit dem Typ „Monospace“ fügen Sie eine Zeile mit drei Backticks (`) hinzu. Geben Sie den Text ein, der mit dem Typ „Monospace“ angezeigt werden soll. Fügen Sie anschließend eine weitere neue Zeile mit drei Backticks hinzu. Das folgende Beispiel zeigt Text, der in der Anzeige mit dem Typ „Monospace“ formatiert wird:

```
```
This appears in a text box with a background shading.
The text is in monospace.
```
```

Überschriften

Zum Erstellen von Überschriften verwenden Sie das Pfundzeichen (#). Ein einzelnes Pfundzeichen und ein Leerzeichen zeigen eine Überschrift der obersten Ebene an. Zwei Pfundzeichen erstellen eine Überschrift der zweiten Ebene. Drei Pfundzeichen erstellen eine Überschrift der dritten Ebene. Die folgenden Beispiele zeigen eine Überschrift der obersten Ebene, der zweiten Ebene und der dritten Ebene:

```
# Top-level heading
```

```
## Second-level heading
```

```
### Third-level heading
```

Textformatierung

Zur Kursiv-Formatierung eines Texts geben Sie auf beiden Seiten des Texts einen einzelnen Unterstrich (_) oder ein einzelnes Sternchen (*) ein.

```
*This text appears in italics.*
```

Zur Fett-Formatierung eines Texts geben Sie auf beiden Seiten des Texts zwei Unterstriche oder Sternchen ein.

```
**This text appears in bold.**
```

Zum Durchstreichen eines Texts geben Sie auf beiden Seiten des Texts zwei Tilden (~) ein.

```
~~This text appears in strikethrough.~~
```

Links

Zum Hinzufügen eines Text-Hyperlinks geben Sie den Text des Links in eckigen Klammern ([ ]) ein, gefolgt von der vollständigen URL in Klammern (( )), wie im folgenden Beispiel gezeigt:

```
Choose [link_text](http://my.example.com).
```

Listen

Zur Formatierung von Zeilen als Teil einer Aufzählungsliste fügen Sie diese in getrennten Zeilen ein, die mit einem einzelnen Sternchen (*) gefolgt von einem Leerzeichen beginnen, wie im folgenden Beispiel gezeigt:

```
Here is a bulleted list:
* Ant
* Bug
* Caterpillar
```

Zur Formatierung von Zeilen als Teil einer nummerierten Liste fügen Sie diese in getrennten Zeilen ein, die mit einer Nummer, einem Punkt (.) und einem Leerzeichen beginnen, wie im folgenden Beispiel gezeigt:

```
Here is a numbered list:
1. Do the first step
2. Do the next step
3. Do the final step
```

Tabellen und Schaltflächen (CloudWatch Dashboards)

CloudWatch Text-Widgets für Dashboards unterstützen Markdown-Tabellen und -Schaltflächen.

Zum Erstellen einer Tabelle trennen Sie Spalten durch vertikale Balken (|) und Zeilen durch neue Zeilen. Wenn Sie die erste Zeile zur Kopfzeile machen möchten, fügen Sie eine Zeile zwischen der Kopfzeile und der ersten Zeile mit Werten ein. Fügen Sie anschließend für jede Spalte in der Tabelle mindestens drei Bindestriche (-) hinzu. Trennen Sie Spalten mit vertikalen Balken. Das folgende Beispiel zeigt den Markdown für eine Tabelle mit zwei Spalten, einer Kopfzeile und zwei Datenzeilen:

```
Table | Header
```

```
----|-----
Amazon Web Services | AWS
1 | 2
```

Mit dem Markdown-Text im vorherigen Beispiel wird die folgende Tabelle erstellt:

Tabelle	Kopfzeile
Amazon Web Services	AWS
1	2

In einem CloudWatch Dashboard-Text-Widget können Sie einen Hyperlink auch so formatieren, dass er als Schaltfläche angezeigt wird. Zum Erstellen einer Schaltfläche verwenden Sie `[button:`*`Button text`*`]` gefolgt von der vollständigen URL in Klammern (( )), wie im folgenden Beispiel gezeigt:

```
[button:Go to AWS](http://my.example.com)
[button:primary:This button stands out even more](http://my.example.com)
```

Fehlerbehebung

In diesem Abschnitt finden Sie Lösungen für häufig auftretende Probleme mit dem AWS Management Console.

Mit Amazon Q Developer können Sie auch häufig auftretende Fehler für einige AWS Services diagnostizieren und beheben. Weitere Informationen finden Sie unter Diagnose häufiger Fehler in der Konsole mit Amazon Q Developer im Amazon Q Developer User Guide.

Themen

Die Seite wird nicht ordnungsgemäß geladen.

- Wenn dieses Problem nur gelegentlich auftritt, überprüfen Sie Ihre Internetverbindung. Versuchen Sie, eine Verbindung über ein anderes Netzwerk oder mit oder ohne VPN herzustellen, oder versuchen Sie es mit einem anderen Webbrowser.
- Wenn alle betroffenen Benutzer demselben Team angehören, kann es sich um eine Browsererweiterung zum Schutz der Privatsphäre oder um ein Problem mit der Sicherheitsfirewall handeln. Browsererweiterungen und Sicherheitsfirewalls können den Zugriff auf die von der verwendeten Domains blockieren. AWS Management Console Versuchen Sie, diese Erweiterungen zu deaktivieren oder die Firewall-Einstellungen anzupassen. Um Probleme mit Ihrer Verbindung zu überprüfen, öffnen Sie die Entwicklertools Ihres Browsers (Chrome, Firefox), und überprüfen Sie die Fehler auf der Registerkarte Konsole. Das AWS Management Console verwendet die Suffixe von Domains, einschließlich der folgenden Liste. Diese Liste ist nicht umfassend und kann sich mit der Zeit ändern. Die Suffixe dieser Domains werden nicht ausschließlich von AWS verwendet.
  - .a2z.com

- .amazon.com
- .amazonaws.com
- .aws
- .aws.com
- .aws.dev
- .awscloud.com
- .awsplayer.com
- .awsstatic.com
- .cloudfront.net
- .live-video.net

> **Warning**
>
> Seit dem 31. Juli 2022 wird Internet Explorer AWS 11 nicht mehr unterstützt. Wir empfehlen Ihnen, den AWS Management Console mit anderen unterstützten Browsern zu verwenden. Weitere Informationen finden Sie im AWS News Blog.

Mein Browser zeigt die Fehlermeldung „Zugriff verweigert“ an, wenn ich eine Verbindung zum AWS Management Console

Kürzlich an der Konsole vorgenommene Änderungen können sich auf Ihren Zugriff auswirken, wenn Sie alle der folgenden Optionen verwenden:

- Ein Browser aus einer VPC.
- VPC-Endpunkte.
- IAM-Richtlinien, die einen `aws:SourceIp` globalen Bedingungsschlüssel enthalten.

Rufen Sie in der Konsole die Seite mit den IAM-Richtlinien auf. Wir empfehlen Ihnen, die IAM-Richtlinien zu überprüfen, die einen `aws:SourceIp` globalen Bedingungsschlüssel und einen Schlüssel hinzufügen `aws:SourceVpc` enthalten.

Alternativ können Sie erwägen, die AWS Management Console Private Access-Funktion zu nutzen, um AWS Management Console über einen VPC-Endpunkt darauf zuzugreifen und die

`aws:SourceVpc` Bedingungen in Ihren Richtlinien zu verwenden. Weitere Informationen finden Sie unter AWS Management Console Privater Zugang.

Mein Browser zeigt Timeout-Fehler an, wenn ich eine Verbindung mit dem AWS Management Console

Wenn in Ihrer Standardeinstellung ein Dienstausfall vorliegt AWS-Region, zeigt Ihr Browser möglicherweise einen 504-Gateway-Timeout-Fehler an, wenn Sie versuchen, eine Verbindung zum herzustellen. AWS Management Console Um sich AWS Management Console von einer anderen Region aus bei der anzumelden, geben Sie in der URL einen alternativen regionalen Endpunkt an. Wenn es zum Beispiel einen Ausfall in der Region `us-west-1` (Nordkalifornien) gibt, verwenden Sie folgende Vorlage für den Zugriff auf die Region `us-west-2` (Oregon):

```
https://region-code.console.aws.amazon.com
```

Weitere Informationen finden Sie unter AWS Management Console -Service-Endpunkte in der Allgemeine AWS-Referenz.

Informationen zum Status aller Dateien AWS-Services, einschließlich der AWS Management Console, finden Sie unter AWS Health Dashboard.

Ich möchte die Sprache der AWS Management Console ändern, kann aber das Sprachauswahlmenü unten auf der Seite nicht finden.

Das Sprachauswahlmenü wurde auf die neue Seite „Unified Settings“ (Einheitliche Einstellungen) verschoben. Um die Sprache von zu ändern AWS Management Console, navigieren Sie zur Seite „Vereinheitlichte Einstellungen“ und wählen Sie dann die Sprache für die Konsole aus.

Weitere Informationen finden Sie unter Ändern der Sprache der AWS Management Console.

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen für das Handbuch „Erste Schritte mit der AWS Management Console ab März 2021 aufgelistet.

Änderung	Beschreibung	Datum
Chatten Sie mit Amazon Q	Eine neue Einstellungsseite, auf der detailliert beschrieben wird, wie Benutzer AWS Fragen an Amazon Q Developer stellen können. Weitere Informationen finden Sie unter Chat mit Amazon Q Developer.	29. Mai 2024
Meine Bewerbungen	Eine neue Seite, die MyApplications vorstellt. Weitere Informationen finden Sie unter Worauf läuft MyApplications? AWS.	29. November 2023
Konfigurieren der einheitlichen Einstellungen	Eine neue Seite mit Einstellungen für die Konfiguration von Einstellungen und Standards, die für den aktuellen Benutzer gelten, einschließlich Sprache und Region. Weitere Informationen finden Sie unter Konfigurieren der einheitlichen Einstellungen.	6. April 2022
Neue AWS Console Home Benutzeroberfläche	Neue AWS Console Home Benutzeroberfläche, die Widgets zur Anzeige wichtiger Nutzungsinformationen und Verknüpfungen zu AWS	25. Februar 2022

Änderung	Beschreibung	Datum
	Diensten enthält. Weitere Informationen finden Sie unter Arbeiten mit Widgets.	
Ändern der Konsolensprache	Auswahl einer anderen Sprache für die AWS Management Console. Weitere Informationen finden Sie unter Ändern der Sprache der AWS Management Console.	01. April 2021
Wird gestartet CloudShell	Öffnen Sie AWS CloudShel l über die AWS CLI-Befehle AWS Management Console und führen Sie sie aus. Weitere Informationen finden Sie unter Starten AWS CloudShell.	22. März 2021

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

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.