Benutzerhandbuch

AWS CloudShell

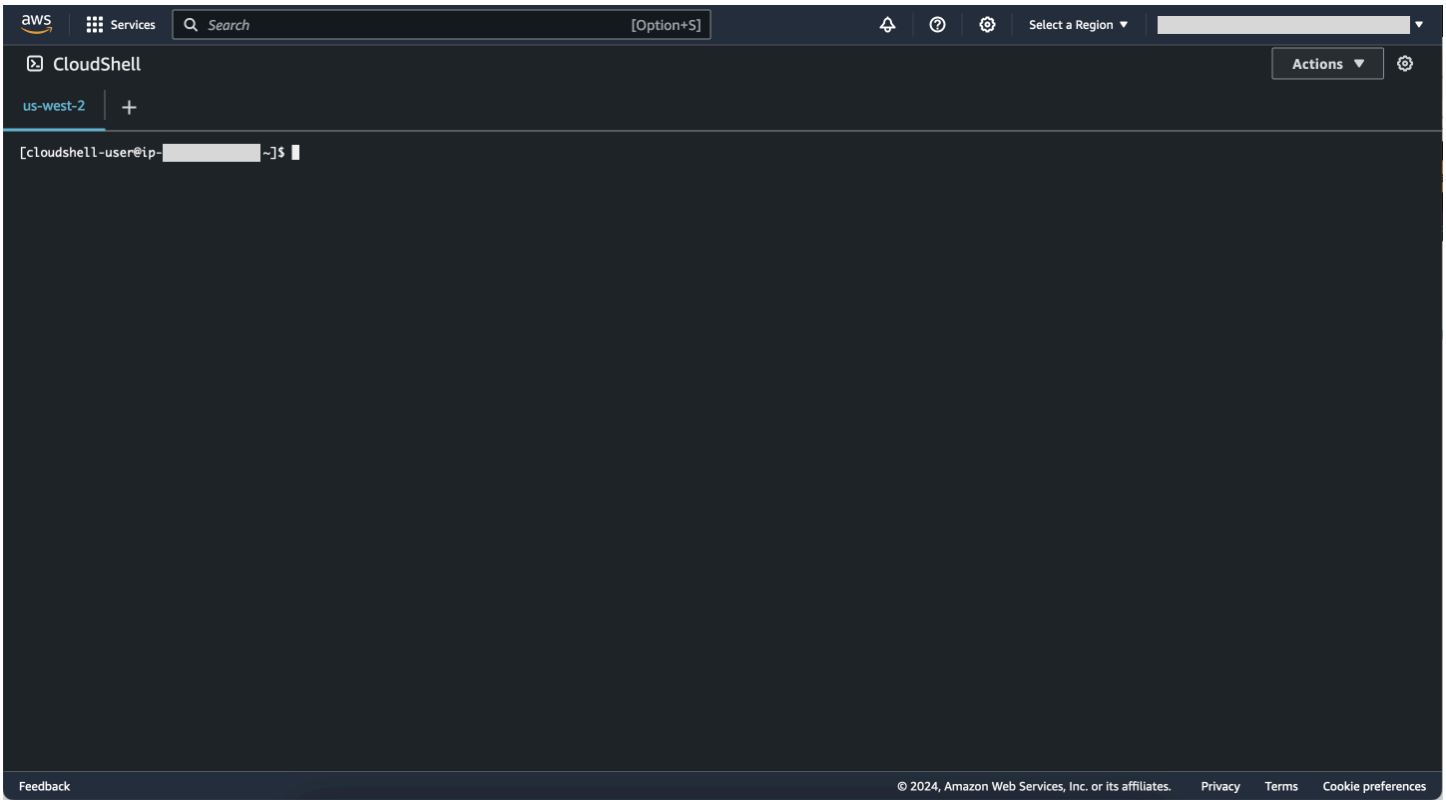
AWS CloudShell: Benutzerhandbuch

Table of Contents

Was ist AWS CloudShell?

AWS CloudShell ist eine browserbasierte, vorauthentifizierte Shell, die Sie direkt von der aus starten können. AWS Management Console Sie können auf verschiedene Arten CloudShell zu ihr navigieren. AWS Management Console Weitere Informationen finden Sie unter Erste Schritte mit AWS CloudShell

Sie können AWS CLI Befehle mit Ihrer bevorzugten Shell ausführen, z. B. Bash PowerShell, oderZ shell. Und Sie können dies tun, ohne Befehlszeilentools herunterzuladen oder zu installieren.



Beim Start AWS CloudShell wird eine Rechenumgebung erstellt, die auf Amazon Linux 2023 basiert. In dieser Umgebung können Sie auf eine Vielzahl vorinstallierter Entwicklungstools, Optionen für das Hoch - und Herunterladen von Dateien sowie auf Dateispeicher zugreifen, der zwischen den Sitzungen bestehen bleibt.

(Probieren Sie es jetzt aus:) Erste Schritte mit AWS CloudShell

AWS CloudShell features

In diesem Thema wird beschrieben, wie Sie CloudShell von der Konsole aus starten, nahtlos zwischen Ihren bevorzugten Befehlszeilen-Shells wechseln und genau CloudShell nach Ihren Wünschen anpassen können. Darüber hinaus können Sie jeweils bis zu 1 GB persistenten Speicher verwenden und erfahren AWS-Region, wie die CloudShell Umgebung durch spezielle Sicherheitsfunktionen geschützt wird.

AWS Command Line Interface

Sie können AWS CloudShell von der aus starten AWS Management Console. Die AWS Anmeldeinformationen, mit denen Sie sich bei der Konsole angemeldet haben, sind automatisch in einer neuen Shell-Sitzung verfügbar. Da AWS CloudShell Benutzer vorab authentifiziert sind, müssen Sie keine Anmeldeinformationen konfigurieren, wenn Sie AWS-Services mit AWS CLI Version 2 interagieren. Das AWS CLI ist in der Rechenumgebung der Shell vorinstalliert.

Weitere Hinweise zur Interaktion mit der AWS-Services Befehlszeilenschnittstelle finden Sie unterZusammenarbeit mitAWS Diensten inAWS CloudShell.

Shells und Entwicklungstools

Mit der Shell, die für AWS CloudShell Sitzungen erstellt wurde, können Sie nahtlos zwischen Ihren bevorzugten Befehlszeilen-Shells wechseln. Insbesondere können Sie zwischen Bash PowerShell, und wechselnZ shell. Sie haben auch Zugriff auf vorinstallierte Tools und Dienstprogramme. Dazu gehörengit,make, pipsudo,tar,tmux, vimwget, undzip.

Die Shell-Umgebung ist vorkonfiguriert und unterstützt mehrere führende Softwaresprachen wie Node.js undPython. Das bedeutet, dass Sie beispielsweise Python Projekte ausführen Node.js können, ohne zuerst Runtime-Installationen durchzuführen. PowerShell Benutzer können die .NET Core Runtime verwenden.

Sie können Dateien, die in einem lokalen Repository erstellt oder AWS CloudShell dorthin hochgeladen wurden, übertragen, bevor Sie diese Dateien in ein Remote-Repository übertragen, das von verwaltet wird AWS CodeCommit.

Weitere Informationen finden Sie unter AWS CloudShellRechenumgebung: Spezifikationen und Software.

Persistenter Speicher

Mit AWS CloudShell können Sie jeweils AWS-Region bis zu 1 GB persistenten Speicher ohne zusätzliche Kosten verwenden. Der persistente Speicher befindet sich in Ihrem Home-Verzeichnis (`$HOME`) und ist für Sie privat. Im Gegensatz zu kurzlebigen Umgebungsressourcen, die nach dem Ende jeder Shell-Sitzung wiederverwendet werden, bleiben Daten in Ihrem Basisverzeichnis zwischen den Sitzungen bestehen.

Weitere Hinweise zur Aufbewahrung von Daten im persistenten Speicher finden Sie unter. Persistenter Speicher

> **Note**
>
> CloudShell VPC-Umgebungen haben keinen persistenten Speicher. Das $HOME-Verzeichnis wird gelöscht, wenn Ihre VPC-Umgebung das Zeitlimit überschreitet (nach 20-30 Minuten Inaktivität) oder wenn Sie Ihre Umgebung löschen oder neu starten.

CloudShell VPC-Umgebungen

AWS CloudShell Mit einer Virtual Private Cloud (VPC) können Sie eine CloudShell Umgebung in Ihrer VPC erstellen. Für jede VPC-Umgebung können Sie eine VPC zuweisen, ein Subnetz hinzufügen und eine oder mehrere Sicherheitsgruppen zuordnen. AWS CloudShell erbt die Netzwerkkonfiguration der VPC und ermöglicht Ihnen die AWS CloudShell sichere Nutzung innerhalb desselben Subnetzes wie andere Ressourcen in der VPC.

Sicherheit

Die AWS CloudShell Umgebung und ihre Benutzer sind durch spezielle Sicherheitsfunktionen geschützt. Dazu gehören Funktionen wie die Verwaltung von IAM-Berechtigungen, Einschränkungen für Shell-Sitzungen und Safe Paste für die Texteingabe.

Verwaltung von Berechtigungen mit IAM

Als Administrator können Sie AWS CloudShell Benutzern mithilfe von IAM-Richtlinien Berechtigungen gewähren oder verweigern. Sie können auch Richtlinien erstellen, die die bestimmten Aktionen spezifizieren, die Benutzer in der Shell-Umgebung ausführen können. Weitere Informationen finden Sie unter AWS CloudShell Zugriff und Nutzung mit IAM-Richtlinien verwalten.

Verwaltung von Shell-Sitzungen

Inaktive und lang andauernde Sitzungen werden automatisch gestoppt und wiederverwendet. Weitere Informationen finden Sie unter Shell-Sitzungen.

Sicheres Einfügen für die Texteingabe

Safe Paste ist standardmäßig aktiviert. Für diese Sicherheitsfunktion müssen Sie sicherstellen, dass der mehrzeilige Text, den Sie in die Shell einfügen möchten, keine schädlichen Skripts enthält. Weitere Informationen finden Sie unter Verwenden von Safe Paste für mehrzeiligen Text.

Optionen zur Anpassung

Sie können Ihr AWS CloudShell Erlebnis genau an Ihre Vorlieben anpassen. Sie können beispielsweise die Bildschirmlayouts (mehrere Tabs) und die angezeigten Textgrößen ändern und zwischen den hellen und dunklen Benutzeroberflächenthemen wechseln. Weitere Informationen finden Sie unter Anpassen IhresAWS CloudShellErfahrung.

Sie können Ihre Shell-Umgebung auch erweitern, indem Sie Ihre eigene Software installieren und Start-Shell-Skripts ändern.

Wiederherstellung der Sitzung

Die Funktion zur Sitzungswiederherstellung stellt Sitzungen wieder her, die Sie über einzelne oder mehrere Browser-Tabs im CloudShell Terminal ausgeführt haben. Wenn Sie kürzlich geschlossene Browser-Tabs aktualisieren oder erneut öffnen, setzt diese Funktion die Sitzung fort, bis die Shell aufgrund einer inaktiven Sitzung beendet wird. Um Ihre CloudShell Sitzung weiter zu verwenden, drücken Sie eine beliebige Taste im Terminalfenster. Weitere Informationen zu Shell-Sitzungen finden Sie unter Shell-Sitzungen.

Bei der Sitzungswiederherstellung werden auch die neuesten Terminalausgaben und laufenden Prozesse auf den einzelnen Terminalregisterkarten wiederhergestellt.

> **Note**
>
> Die Sitzungswiederherstellung ist in mobilen Anwendungen nicht verfügbar.

Preisgestaltung für AWS CloudShell

AWS CloudShell ist eine AWS-Service , die ohne zusätzliche Kosten erhältlich ist. Sie zahlen jedoch für andere AWS Ressourcen, mit denen Sie arbeiten AWS CloudShell. Darüber hinaus gelten auch

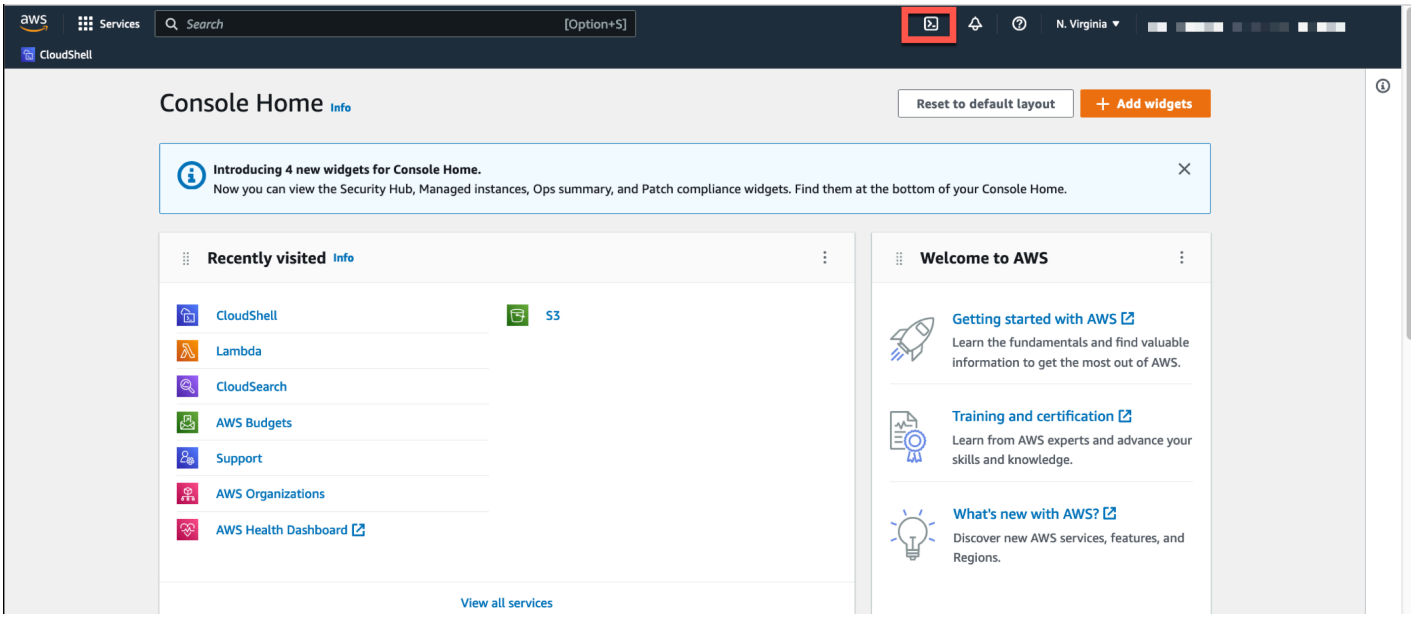
die Standardtarife für Datenübertragungen. Weitere Informationen finden Sie unter AWS CloudShell Preise.

Weitere Informationen finden Sie unter Servicekontingente und Einschränkungen für AWS CloudShell.

Wie fange ich an mit AWS CloudShell?

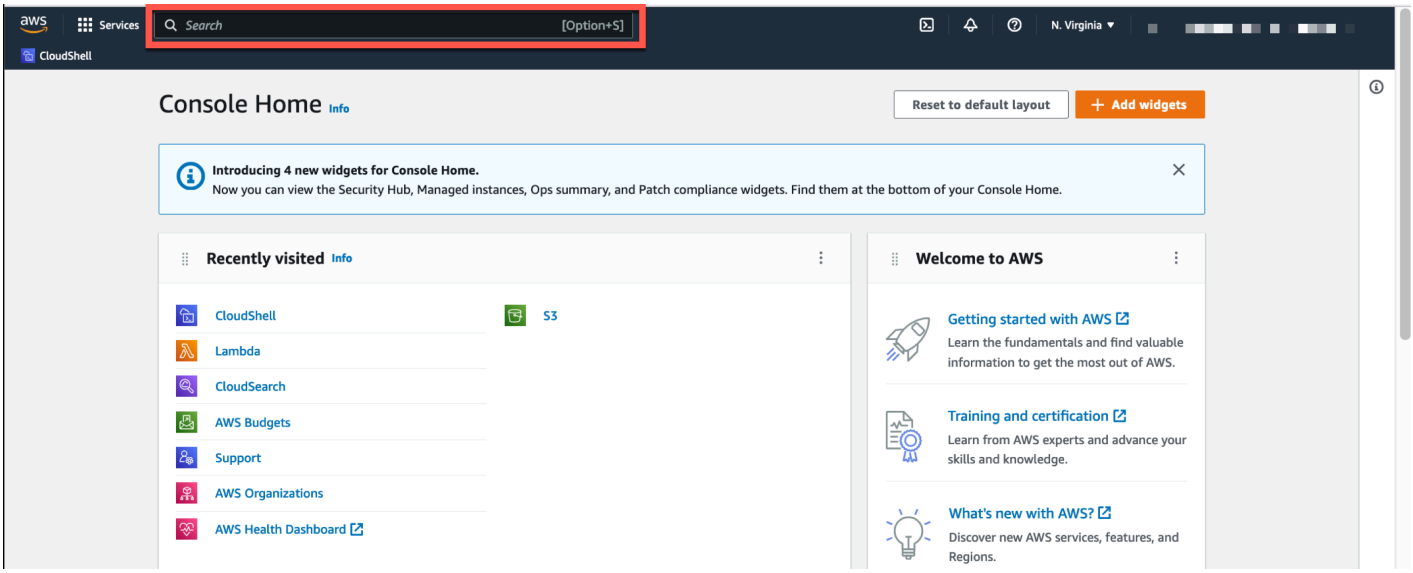
Um mit der Arbeit mit der Shell zu beginnen, melden Sie sich bei der an AWS Management Console und wählen Sie eine der folgenden Optionen:

- Wählen Sie in der Navigationsleiste das CloudShellSymbol aus.



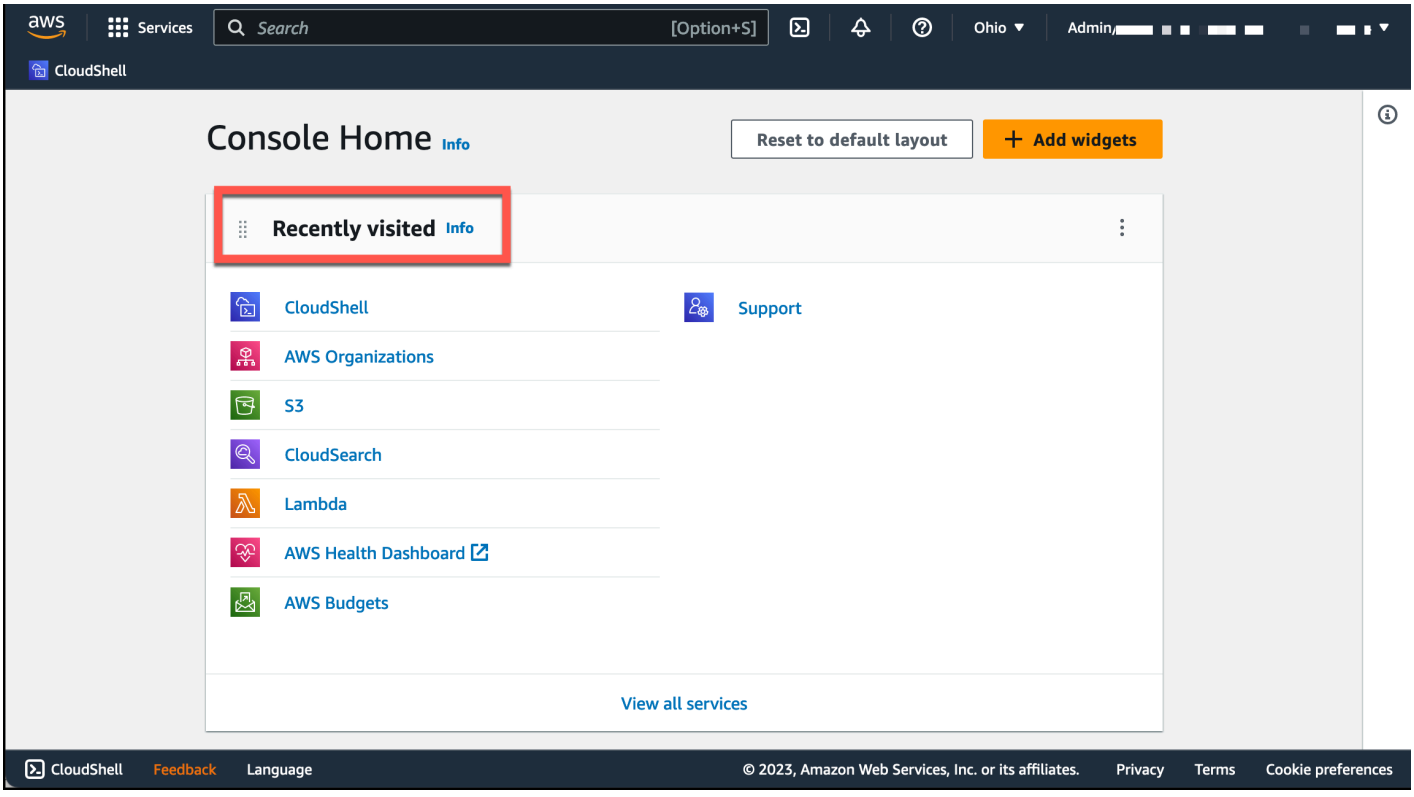
- Geben Sie in das Suchfeld „CloudShell“ ein und wählen Sie dann CloudShell.

  Mit diesem Schritt wird Ihre CloudShell Sitzung im Vollbildmodus geöffnet.

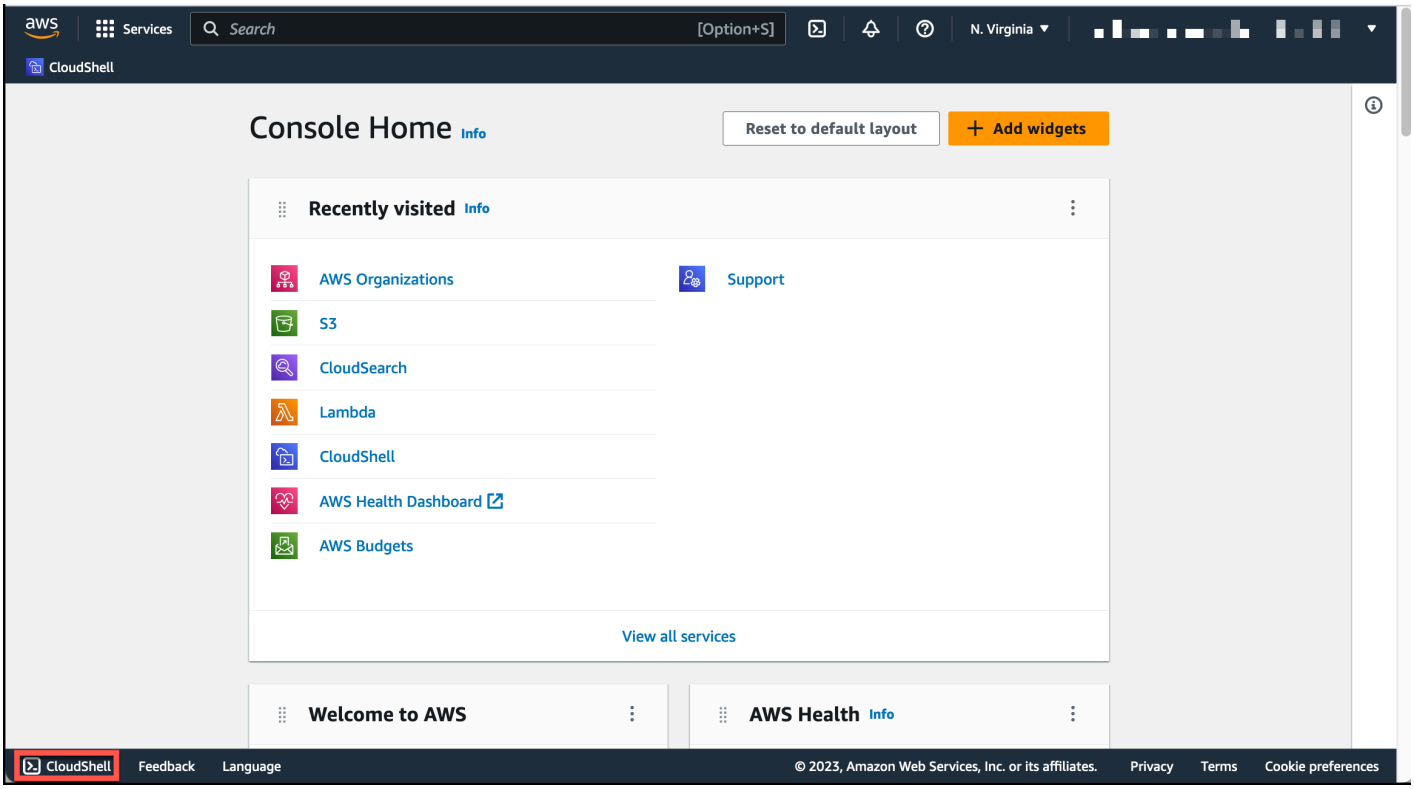


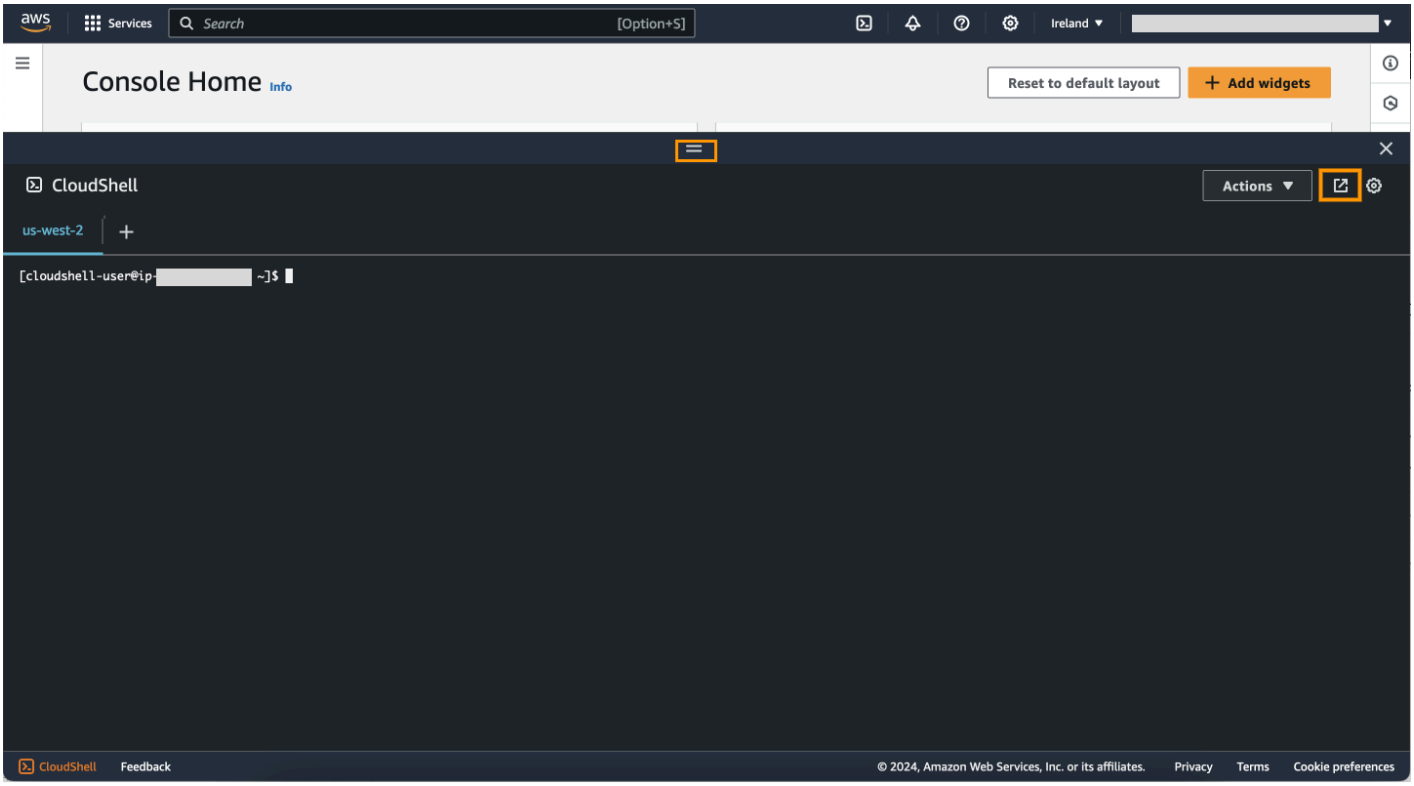
- Wählen Sie im Widget „Kürzlich besucht“ CloudShell.

  Dieser Schritt öffnet Ihre CloudShell Sitzung im Vollbildmodus.



- Wählen Sie CloudShellauf derConsole Toolbar, unten links auf der Konsole. Sie können die Höhe Ihrer CloudShell Sitzung durch Ziehen = anpassen.





Sie können Ihre CloudShell Sitzung auch auf den Vollbildmodus umschalten, indem Sie auf In neuem Browser-Tab öffnen klicken.

Anweisungen zur Anmeldung bei AWS Management Console und zur Ausführung wichtiger Aufgaben finden Sie AWS CloudShell unter Erste Schritte mit AWS CloudShell.

Die wichtigsten AWS CloudShell Themen

- Erste Schritte mit AWS CloudShell
- Arbeiten mit AWS CloudShell
- Zusammenarbeit mitAWS Diensten inAWS CloudShell
- Anpassen IhresAWS CloudShellErfahrung
- AWS CloudShellRechenumgebung: Spezifikationen und Software

AWS CloudShell Häufig gestellte Fragen

Im Folgenden finden Sie Antworten auf einige häufig gestellte Fragen zu AWS CloudShell.

Weitere häufig gestellte Fragen zum Thema Sicherheit finden Sie unterAWS CloudShell Häufig gestellte Fragen zur Sicherheit.

- Wie fange ich an zu verwenden AWS CloudShell?
- Worauf muss ich zugreifen AWS CloudShell?
- Was ist AWS CloudShell auf derConsole Toolbar?
- Wie starte ich AWS CloudShell auf demConsole Toolbar?
- Wie erstelle und verwalte ich meine AWS CloudShell Umgebung?
- Welches AWS-Regionen ist AWS CloudShell verfügbar in?
- Was AWS-Region wird zugewiesen, wenn es in der ausgewählten Region nicht AWS CloudShell verfügbar ist, wenn Sie CloudShell am startenConsole Toolbar?
- In welchen Arten von Muscheln kann ich sie verwenden AWS CloudShell?
- Mit welchen Webbrowsern kann ich sie verwenden AWS CloudShell?
- Welche Webbrowser kann ich verwenden, wenn ich AWS CloudShell auf dem starteConsole Toolbar?
- Kann ich eine Datei herunterladen, wenn ich AWS CloudShell auf dem starteConsole Toolbar?
- Welche Software ist in meiner Shell-Umgebung vorinstalliert?

- Kann ich Software installieren, die in der Shell-Umgebung nicht verfügbar ist?
- Kann ich die Aktionen einschränken, die Benutzer ausführen können AWS CloudShell?
- Wie kann ich Daten aus meinem Home-Verzeichnis verschieben, wenn ich den Speicherort ändern möchte AWS-Region , den ich verwende AWS CloudShell?
- Kann ich das Limit erhöhen, das festlegt, wann aufgrund von Benutzerinaktivität ein AWS CloudShell Timeout eintritt?
- Kann ich vom Startbildschirm AWS Console Mobile Application aus darauf zugreifen AWS CloudShell ?
- Wie kann ich AWS CloudShell in der starten AWS Console Mobile Application?
- Kann ich Sondertasten auf meinen IOS- und Android-Tastaturen verwenden, wenn ich sie AWS CloudShell in der verwende? AWS Console Mobile Application
- Kann ich die AWS CloudShell Tab-Anzeige auf dem in mehrere Tabs aufteilen? AWS Console Mobile Application
- Kann ich AWS CloudShell auf einem Mobilgerät über die Konsolen-Symbolleiste darauf zugreifen?
- Wie hoch sind meine laufenden Kosten CloudShell für meine Amazon VPC?
- Kann ich beantragen, dass das Limit für die Erstellung von VPC-Umgebungen pro IAM-Principal auf mehr als zwei erhöht wird?

Wie fange ich an zu verwenden? AWS CloudShell

Sie können loslegen, indem Sie AWS CloudShell in wenigen Schritten von der aus starten AWS Management Console. Melden Sie sich dazu mit Ihren AWS-Konto oder Ihren IAM-Anmeldeinformationen unter https://console.aws.amazon.com/console/home bei der Konsole an.

Weitere Informationen finden Sie unter Erste Schritte mit AWS CloudShell.

Worauf muss ich zugreifen AWS CloudShell?

Da Sie über den AWS CloudShell zugreifen AWS Management Console, müssen Sie ein IAM-Benutzer sein, der einen gültigen Kontoalias oder eine gültige Konto-ID, einen Benutzernamen und ein Passwort angeben kann.

Um AWS CloudShell auf der Konsole zu starten, benötigen Sie die IAM-Berechtigungen, die in der beigefügten Richtlinie enthalten sind. Weitere Informationen finden Sie unter AWS CloudShell Zugriff und Nutzung mit IAM-Richtlinien verwalten.

Was ist AWS CloudShell auf demConsole Toolbar?

Das CloudShell Symbol unten links auf dem AWS Management Console.

Wie starte ich AWS CloudShell auf demConsole Toolbar?

Sie können AWS CloudShell auf dem starten, Console Toolbar indem Sie das CloudShellSymbol unten links auf der Konsole auswählen.

Welches AWS-Regionen ist AWS CloudShell verfügbar in?

Eine Liste der unterstützten AWS-Regionen und der zugehörigen Dienstendpunkte finden Sie AWS CloudShell auf der Seite im Allgemeine Amazon Web Services-Referenz.

Welcher AWS-Region wird zugewiesen, wenn er in der ausgewählten Region nicht AWS CloudShell verfügbar ist, wenn Sie CloudShell auf dem Console Toolbar starten?

Die Standardregion ist einer Region zugewiesen, die der ausgewählten Region am nächsten liegt. Weitere Informationen finden Sie unter Wählen Sie eine Region aus AWS CloudShell, starten Sie und wählen Sie eine Shell aus.

Sie können den Befehl ausführen, der Berechtigungen zur Verwaltung von Ressourcen in einer anderen Region als der Standardregion bereitstellt. Weitere Informationen finden Sie unter Arbeiten in AWS-Regionen.

In welchen Arten von Muscheln kann ich sie verwenden AWS CloudShell?

AWS CloudShell In können Sie Befehle mit dem Bash shell PowerShell, oder dem ausführenZ shell. Um zwischen den Shells zu wechseln, geben Sie den Shell-Namen, den Sie verwenden möchten, in der Befehlszeile im folgenden Format ein:

- `bash`: Verwenden Sie Bash shell
- `pwsh`: Benutze PowerShell
- `zsh`: Benutze die Z shell

Mit welchen Webbrowsern kann ich sie verwenden AWS CloudShell?

AWS CloudShell unterstützt die neuesten Versionen der Browser Google Chrome, Mozilla Firefox, Microsoft Edge und Apple Safari.

Wie erstelle und verwalte ich meine AWS CloudShell Umgebung?

Ihre AWS CloudShell Umgebung wird pro IAM-Benutzer-ID pro Region erstellt und verwaltet. Sie können das überprüfen, `UserId` indem Sie es ausführen`aws sts get-caller-identity`. Die Umgebung gehört der IAM-Benutzer-ID in dieser spezifischen Region. Sie können auf eine andere AWS CloudShell Umgebung zugreifen, wenn Sie die IAM `UserId` oder die Region ändern.

Welche Webbrowser kann ich verwenden, wenn ich AWS CloudShell auf dem Console Toolbar starte?

Sie können Console Toolbar mit den CloudShell neuesten Versionen der Browser Google Chrome, Microsoft Edge, Mozilla Firefox und Apple Safari starten.

Kann ich Dateien von herunterladen AWS CloudShell?

Ja, Sie können eine Datei herunterladen, wenn Sie sie mit einem Browser CloudShell auf der Console Toolbar oder von der CloudShell Konsolenseite aus starten. Sie können eine Datei mit den neuesten Versionen der Browser Google Chrome und Microsoft Edge herunterladen.

Derzeit können Sie eine Datei nicht mit den Browsern Mozilla Firefox und Apple Safari herunterladen.

> **Note**
>
> Die Option zum Herunterladen von Dateien ist für AWS CloudShell VPC-Umgebungen nicht verfügbar.

Welche Software ist in meiner Shell-Umgebung vorinstalliert?

Mit der Shell, die für AWS CloudShell Sitzungen erstellt wurde, können Sie nahtlos zwischen Ihren bevorzugten Befehlszeilen-Shells (Bash PowerShell, und) wechseln. Z shell Sie können auch auf vorinstallierte Tools und Dienstprogramme wieMake,,,, pip sudo tartmux, Vim und zugreifen. Wget Zip

Die Shell-Umgebung ist vorkonfiguriert und unterstützt die meisten wichtigen Softwaresprachen. Sie können sie beispielsweise verwenden, um Python Projekte auszuführenNode.js, ohne zuerst Runtime-Installationen durchführen zu müssen. PowerShell Benutzer können die .NET Core Runtime verwenden.

Sie können Dateien, die mit der Shell erstellt oder mit der Shell-Schnittstelle hochgeladen wurden, zu einem versionskontrollierten Repository hinzufügen, das mit einer vorinstallierten Version von verwaltet wird. git

Weitere Informationen finden Sie unter Vorinstallierte Software.

Kann ich Software installieren, die in der Shell-Umgebung nicht verfügbar ist?

Ja, AWS CloudShell Benutzer haben sudo Rechte und können Software von der Befehlszeile aus installieren. Weitere Informationen finden Sie unter Software von Drittanbietern in Ihrer Shell-Umgebung installieren.

Kann ich die Aktionen einschränken, die Benutzer ausführen können AWS CloudShell?

Ja, Sie können kontrollieren, welche Aktionen Benutzer ausführen können AWS CloudShell. Sie können Benutzern beispielsweise Zugriff gewähren, sie AWS CloudShell aber daran hindern, Dateien innerhalb der Shell-Umgebung hoch- oder herunterzuladen. Alternativ können Sie Benutzer auch vollständig am Zugriff AWS CloudShell hindern. Weitere Informationen finden Sie unter AWS CloudShell Zugriff und Nutzung mit IAM-Richtlinien verwalten.

Wie kann ich Daten aus meinem Home-Verzeichnis verschieben, wenn ich den Speicherort ändern möchte AWS-Region , den ich verwende AWS CloudShell?

Um Ihre AWS CloudShell Daten von einer Region in eine andere AWS-Region zu verschieben, laden Sie zuerst den Inhalt Ihres Home-Verzeichnisses in einer Region auf Ihren lokalen Computer herunter und laden Sie ihn anschließend von dort in das Home-Verzeichnis in einer anderen Region hoch. Weitere Informationen finden Sie unter Tutorial: Kopieren mehrerer Dateien zwischen Ihrem lokalen Computer undAWS CloudShell.

> **Note**
>
> Upload- und Download-Optionen sind für AWS CloudShell VPC-Umgebungen nicht verfügbar.

Kann ich das Limit erhöhen, das festlegt, wann aufgrund von Benutzerinaktivität ein AWS CloudShell Timeout eintritt?

Ihre Shell-Sitzung endet automatisch nach etwa 20 bis 30 Minuten, wenn Sie nicht mit der Tastatur oder dem AWS CloudShell Zeiger interagieren. Laufende Prozesse zählen nicht als Interaktionen. Da CloudShell es für gezielte, aufgabenbasierte Aktivitäten konzipiert ist, gibt es derzeit keine Pläne, dieses Timeout-Limit zu erhöhen.

Wenn Sie terminalbasierte Aufgaben AWS-Service mit flexibleren Timeouts ausführen möchten, empfehlen wir, unsere cloudbasierte IDE zu verwenden oder eine Amazon EC2 AWS Cloud9EC2-Instance zu starten und eine Verbindung zu ihr herzustellen.

Kann ich vom Startbildschirm AWS Console Mobile Application aus darauf zugreifen AWS CloudShell ?

Ja, Sie können darauf zugreifen AWS CloudShell , AWS Console Mobile Application indem Sie sich bei der Console Mobile Application anmelden. Weitere Informationen finden Sie im AWS Console Mobile Application -Benutzerhandbuch.

Wie kann ich AWS CloudShell in der starten AWS Console Mobile Application?

Sie können AWS CloudShell mit einer der folgenden Methoden starten:

1. Wählen Sie das AWS CloudShellSymbol unten in der Navigationsleiste aus.
2. Wählen Sie AWS CloudShellim Menü Dienste die aus.

> **Note**
>
> Derzeit können Sie in der keine VPC-Umgebungen erstellen oder starten. AWS Console Mobile Application

Kann ich Sondertasten auf meinen iOS- und Android-Tastaturen verwenden, wenn ich AWS CloudShell in der? AWS Console Mobile Application

Ja, Sie können Sondertasten auf Ihren iOS- und Android-Tastaturen verwenden. Weitere Informationen finden Sie im AWS Console Mobile Application User Guide.

Kann ich die AWS CloudShell Tab-Anzeige auf dem in mehrere Tabs aufteilen AWS Console Mobile Application?

Nein, derzeit können Sie in Ihrer mobilen Anwendung nicht mehrere AWS CloudShell Tabs ausführen.

Kann ich AWS CloudShellConsole Toolbar auf einem Mobilgerät darauf zugreifen?

Nein, derzeit können Sie AWS CloudShell Console Toolbar auf Ihrem Mobilgerät nicht darauf zugreifen.

Wie hoch sind meine laufenden Kosten CloudShell für meine Amazon VPC?

Es fallen keine Gebühren an, um eine Verbindung zu Ihrer privaten VPC herzustellen und auf die darin enthaltenen Ressourcen zuzugreifen. Datenübertragungen innerhalb Ihrer privaten VPC sind in Ihrer VPC-Abrechnung enthalten, und Datenübertragungen zwischen Ihren VPCs über CloudShell werden zu den gleichen Kosten wie Ihre aktuelle Abrechnung berechnet. CloudShell

Kann ich beantragen, dass das Limit für die Erstellung von VPC-Umgebungen pro IAM-Principal auf mehr als zwei erhöht wird?

Nein, das können Sie nicht. Sie können nur bis zu zwei VPC-Umgebungen erstellen.

Erste Schritte mit AWS CloudShell

In diesem einführenden Tutorial erfahren Sie, wie Sie wichtige Aufgaben mithilfe der Shell-Befehlszeilenschnittstelle starten AWS CloudShell und ausführen.

Zunächst melden Sie sich bei der an AWS Management Console und wählen eine aus AWS-Region. Anschließend öffnen Sie ein neues Browserfenster und einen Shell-Typ, mit dem Sie arbeiten möchten. CloudShell

Als Nächstes erstellen Sie einen neuen Ordner in Ihrem Home-Verzeichnis und laden eine Datei von Ihrem lokalen Computer in diesen Ordner hoch. Sie bearbeiten diese Datei mit einem vorinstallierten Editor, bevor Sie sie als Programm über die Befehlszeile ausführen. Zuletzt rufen Sie AWS CLI Befehle auf, um einen Amazon S3 S3-Bucket zu erstellen und Ihre Datei als Objekt zum Bucket hinzuzufügen.

Voraussetzungen

IAM-Berechtigungen

Sie können Berechtigungen für erhalten, AWS CloudShell indem Sie Ihrer IAM-Identität (z. B. einem Benutzer, einer Rolle oder einer Gruppe) die folgende AWS verwaltete Richtlinie hinzufügen:

- AWSCloudShellFullAccess: Bietet Benutzern vollen Zugriff auf AWS CloudShell und die zugehörigen Funktionen.

In diesem Tutorial interagieren Sie auch mit AWS-Services. Genauer gesagt interagieren Sie mit Amazon S3, indem Sie einen S3-Bucket erstellen und diesem Bucket ein Objekt hinzufügen. Ihre IAM-Identität erfordert eine Richtlinie, die mindestens die `s3:PutObject` Berechtigungen `s3:CreateBucket` und gewährt.

Weitere Informationen finden Sie unter Amazon S3 S3-Aktionen im Amazon Simple Storage Service-Benutzerhandbuch.

Übungsdatei

Diese Übung beinhaltet auch das Hochladen und Bearbeiten einer Datei, die dann als Programm über die Befehlszeilenschnittstelle ausgeführt wird. Öffnen Sie einen Texteditor auf Ihrem lokalen Computer und fügen Sie den folgenden Codeausschnitt hinzu.

```
import sys
x=int(sys.argv[1])
y=int(sys.argv[2])
sum=x+y
print("The sum is",sum)
```

Speichern Sie die Datei mit dem Namen `add_prog.py`.

Inhalt

Schritt 1: Melden Sie sich an AWS Management Console

In diesem Schritt müssen Sie Ihre IAM-Benutzerinformationen eingeben, um auf die AWS Management Console zuzugreifen. Wenn Sie sich bereits in der Konsole befinden, fahren Sie mit Schritt 2 fort.

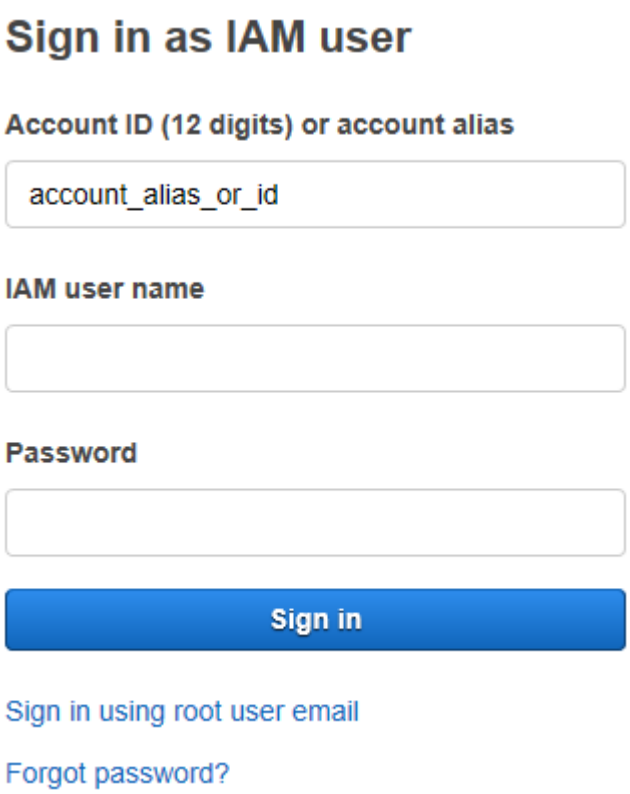
- Sie können auf die zugreifen, AWS Management Console indem Sie die Anmelde-URL eines IAM-Benutzers verwenden oder die Haupt-Anmeldeseite aufrufen.

  IAM user sign-in URL

  - Öffnen Sie einen Browser und geben Sie die folgende Anmelde-URL ein. `account_alias_or_id`Ersetzen Sie es durch den Kontoalias oder die Konto-ID, die Ihr Administrator bereitgestellt hat.

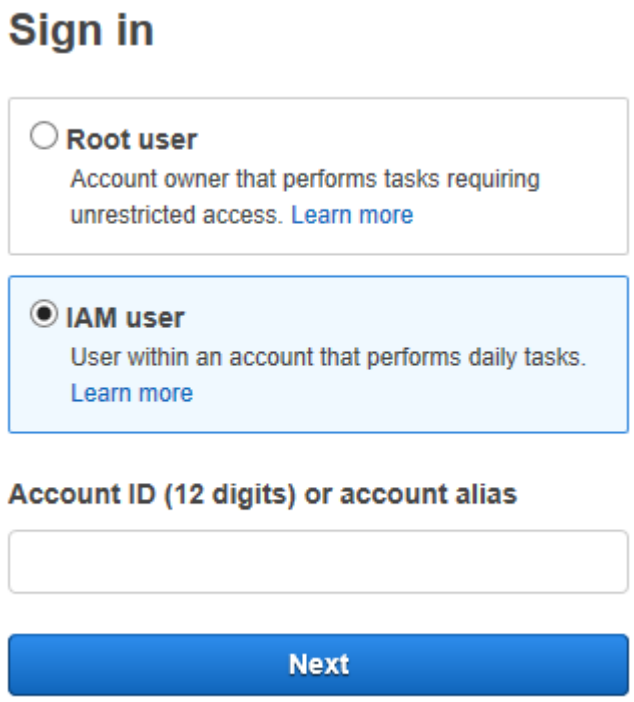
```
https://account_alias_or_id.signin.aws.amazon.com/console/
```

- Geben Sie Ihre IAM-Anmeldeinformationen ein und wählen Sie Anmelden aus.

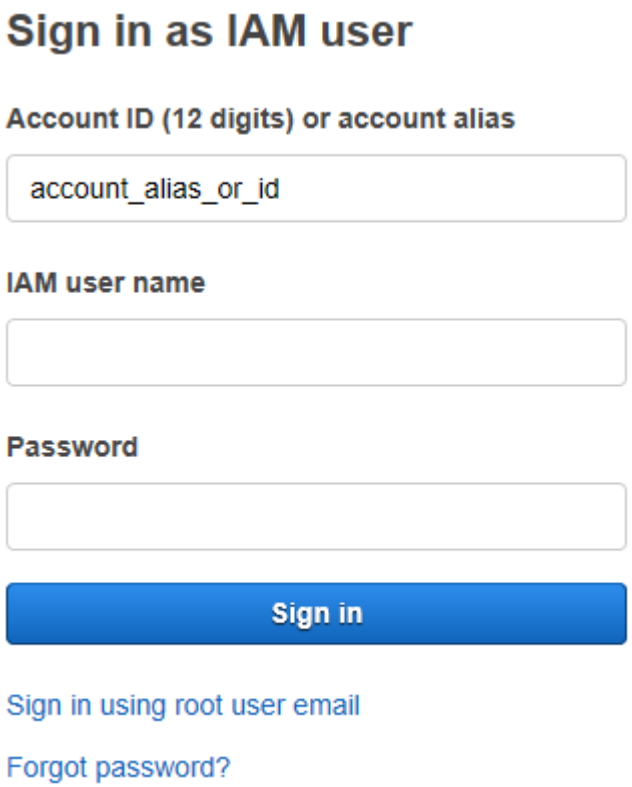


Main sign-in page

- Öffnen Sie https://aws.amazon.com/console/.
- Wenn Sie sich zuvor nicht mit diesem Browser angemeldet haben, wird die Haupt-Anmeldeseite angezeigt. Wählen Sie IAM-Benutzer, geben Sie den Kontoalias oder die Konto-ID ein und klicken Sie auf Weiter.



- Wenn Sie sich bereits zuvor als IAM-Benutzer angemeldet haben. Ihr Browser erinnert sich möglicherweise an den Kontoalias oder die AWS-Konto Konto-ID für. Wenn ja, geben Sie Ihre IAM-Anmeldeinformationen ein und wählen Sie Anmelden.



> **Note**
>
> Sie können sich auch als Root-Benutzer anmelden. Diese Identität hat vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto. Wir empfehlen dringend, den Root-Benutzer nicht für alltägliche Aufgaben zu verwenden, auch nicht für administrative Aufgaben. Folgen Sie stattdessen dem bewährten Verfahren, den Stammbenutzer ausschließlich zur Erstellung des ersten IAM-Benutzers zu verwenden.

Schritt 2: Wählen Sie eine Region aus AWS CloudShell, starten Sie sie und wählen Sie eine Shell

In diesem Schritt starten Sie AWS CloudShell von der Konsolenoberfläche aus, wählen eine verfügbare AWS-Region aus und wechseln zu Ihrer bevorzugten Shell, z. B. Bash PowerShell, oderZ shell.

1. AWS-Region Um eine auszuwählen, in der Sie arbeiten möchten, gehen Sie zum Menü „Region auswählen“ und wählen Sie eine unterstützte AWS Region aus, in der Sie arbeiten möchten. (Verfügbare Regionen sind hervorgehoben.)

> **Important**
>
> Wenn Sie zwischen Regionen wechseln, wird die Benutzeroberfläche aktualisiert und der Name der ausgewählten Region AWS-Region wird über dem Befehlszeilentext angezeigt. Alle Dateien, die Sie dem persistenten Speicher hinzufügen, sind nur in diesem Speicher verfügbar. AWS-Region Wenn Sie die Region wechseln, können Sie auf verschiedene Speicher und Dateien zugreifen.

> **Important**
>
> Wenn die Option in der ausgewählten Region nicht CloudShell verfügbar ist, wenn Sie CloudShell auf demConsole Toolbar, unten links auf der Konsole, starten, dann ist die Standardregion auf eine Region festgelegt, die der ausgewählten Region am nächsten ist. Sie können den Befehl ausführen, der Berechtigungen zum Verwalten

von Ressourcen in einer anderen Region als der Standardregion bereitstellt. Weitere Informationen finden Sie unter Arbeiten in AWS-Regionen.

Example

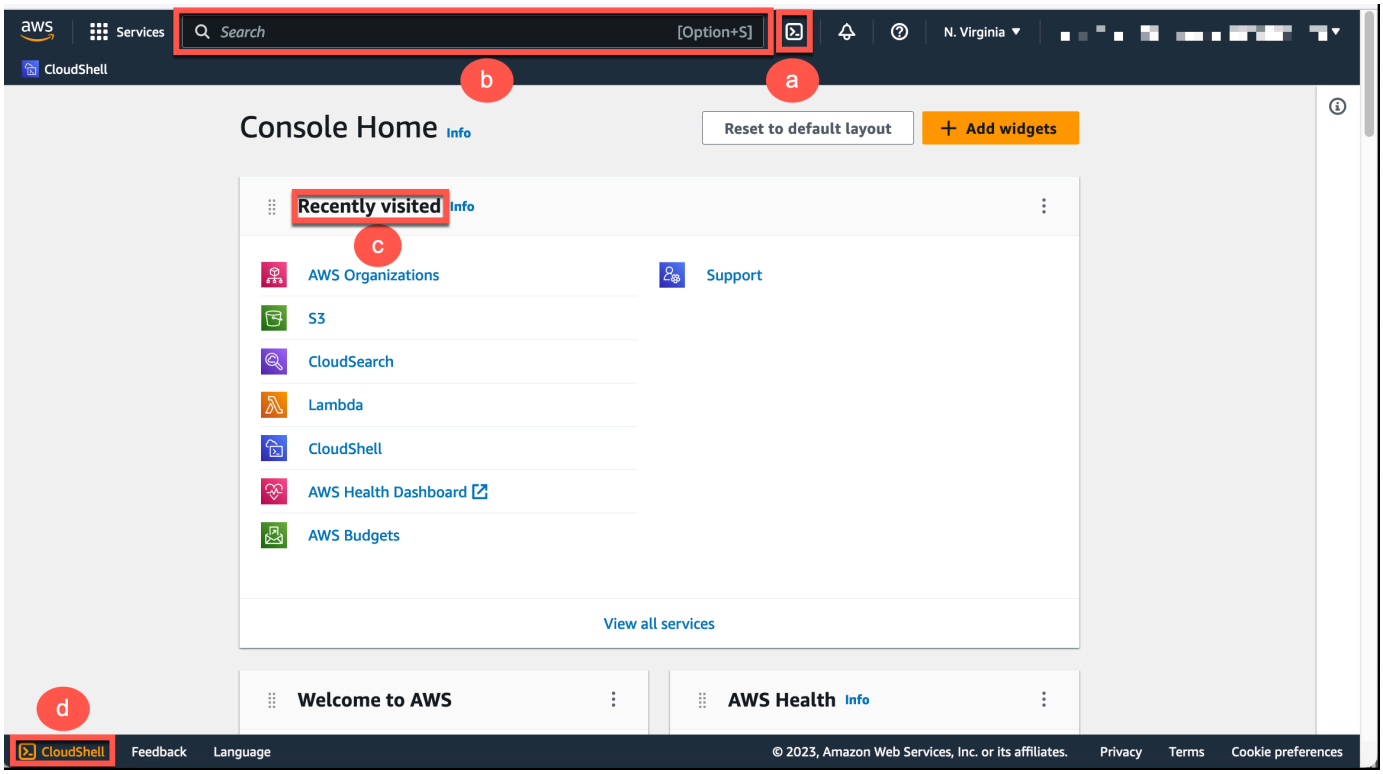
Beispiel

Wenn Sie Europa (Spanien) wählen, eu-south-2 aber in Europa (Spanien) nicht CloudShell verfügbar isteu-south-2, ist die Standardregion auf Europa (Irland) festgelegteu-west-1, was Europa (Spanien) am nächsten isteu-south-2.

Sie verwenden die Servicekontingenten für die Standardregion Europa (Irland) eu-west-1 und dieselbe CloudShell Sitzung wird in allen Regionen wiederhergestellt. Die Standardregion wird möglicherweise geändert und Sie werden im CloudShell Browserfenster darüber informiert.

2. Von der aus können Sie starten AWS Management Console, CloudShell indem Sie eine der folgenden Optionen wählen:

   1. Wählen Sie in der Navigationsleiste das CloudShellSymbol aus.
   2. Geben Sie in das Suchfeld „CloudShell“ ein und wählen Sie dann CloudShell.
   3. Wählen Sie im Widget „Kürzlich besucht“ CloudShell.
   4. Wählen Sie CloudShellauf derConsole Toolbar, unten links auf der Konsole.
      - Um die Höhe Ihrer CloudShell Sitzung anzupassen, ziehen Sie=.
      - Um Ihre CloudShell Sitzung in den Vollbildmodus umzuschalten, klicken Sie auf das Symbol In neuem Browser-Tab öffnen.



Wenn die Eingabeaufforderung angezeigt wird, ist die Shell für die Interaktion bereit.

> **Note**
>
> Wenn Sie auf Probleme stoßen, die Sie daran hindern, erfolgreich zu starten oder mit ihnen zu interagieren AWS CloudShell, suchen Sie nach Informationen zur Identifizierung und Behebung dieser Probleme unterProblembehebung AWS CloudShell.

3. Um eine vorinstallierte Shell auszuwählen, mit der Sie arbeiten möchten, geben Sie ihren Programmnamen an der Befehlszeile ein.

   Bash

   ```
   bash
   ```

   Wenn Sie zu wechselnBash, wird das Symbol in der Befehlszeile auf $ aktualisiert.

> **Note**
>
> Bashist die Standard-Shell, die beim Starten ausgeführt wird AWS CloudShell.

PowerShell

```
pwsh
```

Wenn Sie zu wechseln PowerShell, wird das Symbol in der Befehlszeile auf aktualisiertPS>.

Z shell

```
zsh
```

Wenn Sie zu wechselnZ shell, wird das Symbol in der Befehlszeile auf aktualisiert%.

Informationen zu den in Ihrer Shell-Umgebung vorinstallierten Versionen finden Sie in der Shell-Tabelle im Abschnitt CloudShell AWS-Rechenumgebung.

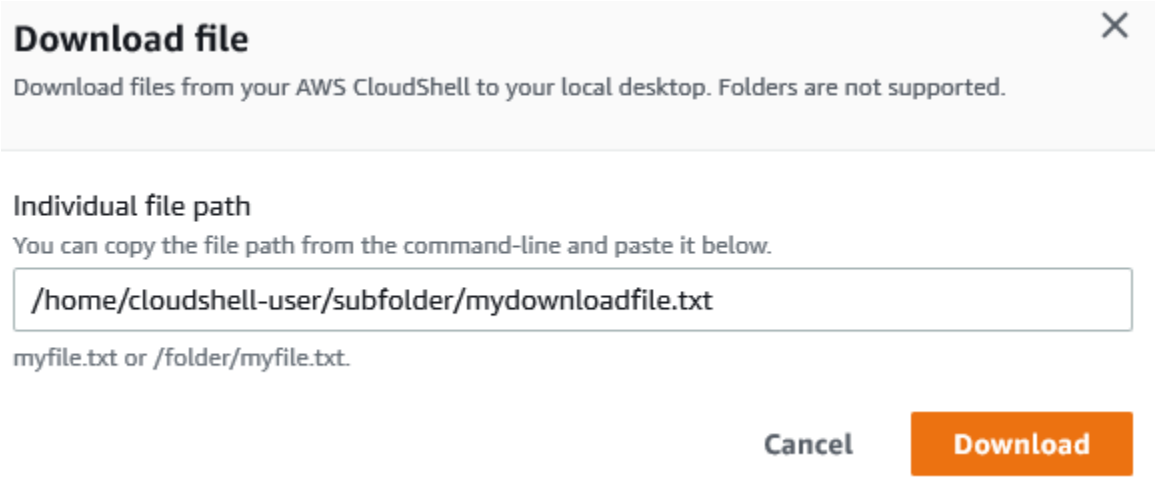
Schritt 3: Laden Sie eine Datei herunter von AWS CloudShell

> **Note**
>
> Diese Option ist für VPC-Umgebungen nicht verfügbar.

Dieser Schritt führt Sie durch den Vorgang des Herunterladens einer Datei.

1. Um eine Datei herunterzuladen, gehen Sie zu Aktionen und wählen Sie im Menü die Option Datei herunterladen.

   Das Dialogfeld „Datei herunterladen“ wird angezeigt.
2. Geben Sie im Dialogfeld Datei herunterladen den Pfad für die Datei ein, die heruntergeladen werden soll.



> **Note**
>
> Sie können absolute oder relative Pfade verwenden, wenn Sie eine Datei zum Herunterladen angeben. Bei relativen Pfadnamen `/home/cloudshell-user/` wird standardmäßig automatisch zum Start hinzugefügt. Um also eine Datei mit dem Namen herunterzuladen`mydownload-file`, sind die beiden folgenden Pfade gültig:
>
> - Absoluter Pfad: `/home/cloudshell-user/subfolder/mydownloadfile.txt`
> - Relativer Pfad: `subfolder/mydownloadfile.txt`

3. Wählen Sie Herunterladen aus.

Wenn der Dateipfad korrekt ist, wird ein Dialogfeld angezeigt. Sie können dieses Dialogfeld verwenden, um die Datei mit der Standardanwendung zu öffnen. Sie können die Datei auch in einem Ordner auf Ihrem lokalen Computer speichern.

> **Note**
>
> Die Download-Option ist nicht verfügbar, wenn Sie CloudShell auf dem startenConsole Toolbar. Sie können eine Datei von der CloudShell Konsole oder mit dem Chrome-Webbrowser herunterladen. Weitere Informationen zum Herunterladen einer Datei finden Sie unter Schritt 3: Datei herunterladen von AWS CloudShell.

Schritt 4: Laden Sie eine Datei hoch auf AWS CloudShell

> **Note**
>
> Diese Option ist für VPC-Umgebungen nicht verfügbar.

In diesem Schritt wird beschrieben, wie Sie eine Datei hochladen und sie dann in ein neues Verzeichnis in Ihrem Home-Verzeichnis verschieben.

1. Um Ihr aktuelles Arbeitsverzeichnis zu überprüfen, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

   ```
   pwd
   ```

   Wenn Sie die Eingabetaste drücken, gibt die Shell Ihr aktuelles Arbeitsverzeichnis zurück (z. B.`/home/cloudshell-user`).
2. Um eine Datei in dieses Verzeichnis hochzuladen, gehen Sie zu Aktionen und wählen Sie im Menü Datei hochladen.

   Das Dialogfeld „Datei hochladen“ wird angezeigt.
3. Wählen Sie Browse.
4. Wählen Sie im Dialogfeld „Datei-Upload“ Ihres Systems die Textdatei aus, die Sie für dieses Tutorial erstellt haben (`add_prog.py`), und klicken Sie auf Öffnen.
5. Wählen Sie im Dialogfeld „Datei hochladen“ die Option Hochladen aus.

   Ein Fortschrittsbalken verfolgt den Upload. Wenn der Upload erfolgreich ist, wird in einer Meldung bestätigt, dass `add_prog.py` er dem Stammverzeichnis Ihres Home-Verzeichnisses hinzugefügt wurde.
6. Um ein Verzeichnis für die Datei zu erstellen, geben Sie den Befehl make directories ein:`mkdir mysub_dir`.
7. Um die hochgeladene Datei vom Stammverzeichnis Ihres Home-Verzeichnisses in das neue Verzeichnis zu verschieben, verwenden Sie den `mv` folgenden Befehl:

   ```
   mv add_prog.py mysub_dir.
   ```
8. Um Ihr Arbeitsverzeichnis in das neue Verzeichnis zu ändern, geben Sie ein`cd mysub_dir`.

Die Befehlszeile wird aktualisiert, um anzuzeigen, dass Sie Ihr Arbeitsverzeichnis geändert haben.

9. Geben Sie den `ls` Befehl ein`mysub_dir`, um den Inhalt des aktuellen Verzeichnisses anzuzeigen.

   Der Inhalt des Arbeitsverzeichnisses wird aufgelistet. Dazu gehört auch die Datei, die Sie gerade hochgeladen haben.

Schritt 5: Entferne eine Datei von AWS CloudShell

In diesem Schritt wird beschrieben, wie Sie eine Datei aus entfernen AWS CloudShell.

1. Um eine Datei zu entfernen AWS CloudShell, verwenden Sie Standard-Shell-Befehle wie `rm` (remove).

   ```
   rm my-file-for-removal
   ```

2. Um mehrere Dateien zu entfernen, die bestimmte Kriterien erfüllen, führen Sie den `find` Befehl aus.

   Im folgenden Beispiel werden alle Dateien entfernt, deren Namen das Suffix „.pdf“ enthalten.

   ```
   find -type f -name '*.pdf' -delete
   ```

> **Note**
>
> Angenommen, Sie beenden die Verwendung AWS CloudShell in einem bestimmten. AWS-Region Anschließend werden die Daten, die sich im persistenten Speicher dieser Region befinden, nach einem bestimmten Zeitraum automatisch entfernt. Weitere Informationen finden Sie unter Persistenter Speicher.

Schritt 6: Erstellen Sie eine Sicherung des Home-Verzeichnisses

1. Erstellen Sie eine Sicherungsdatei

   Erstellen Sie einen temporären Ordner außerhalb des Home-Verzeichnisses.

```
HOME_BACKUP_DIR=$(mktemp --directory)
```

Sie können eine der folgenden Optionen verwenden, um ein Backup zu erstellen:

a. Erstellen Sie eine Sicherungsdatei mit tar

Um eine Sicherungsdatei mit Tar zu erstellen, geben Sie den folgenden Befehl ein:

```
tar \
    --create \
    --gzip \
    --verbose \
    --file=${HOME_BACKUP_DIR}/home.tar.gz \
    [--exclude ${HOME}/.cache] \ // Optional
    ${HOME}/
echo "Home directory backed up to this file: ${HOME_BACKUP_DIR}/home.tar.gz"
```

b. Erstellen Sie eine Sicherungsdatei mit Zip

Um eine Sicherungsdatei mit Zip zu erstellen, geben Sie den folgenden Befehl ein:

```
zip \
    --recurse-paths \
    ${HOME_BACKUP_DIR}/home.zip \
    ${HOME} \
    [--exclude ${HOME}/.cache/\*] // Optional
echo "Home directory backed up to this file: ${HOME_BACKUP_DIR}/home.zip"
```

2. Übertragen Sie die Sicherungsdatei nach draußen CloudShell

Sie können eine der folgenden Optionen verwenden, um die Sicherungsdatei nach außen zu übertragen CloudShell:

a. Laden Sie die Sicherungsdatei auf Ihren lokalen Computer herunter

Sie können die im vorherigen Schritt erstellte Datei herunterladen. Weitere Informationen zum Herunterladen einer Datei von CloudShell finden Sie unter Datei herunterladen von AWS CloudShell.

Geben Sie im Dialogfeld „Datei herunterladen“ den Pfad für die Datei ein, die heruntergeladen werden soll (z. B. `/tmp/tmp.iA99tD9L98/home.tar.gz`).

b. Übertragen Sie die Sicherungsdatei auf S3

Geben Sie den folgenden Befehl ein, um einen Bucket zu generieren:

```
aws s3 mb s3://${BUCKET_NAME}
```

Verwenden Sie AWS CLI, um die Datei in den S3-Bucket zu kopieren:

```
aws s3 cp ${HOME_BACKUP_DIR}/home.tar.gz s3://${BUCKET_NAME}
```

> **Note**
>
> Es können Gebühren für die Datenübertragung anfallen.

3. Direktes Backup in einen S3-Bucket

Um direkt in einem S3-Bucket zu sichern, geben Sie den folgenden Befehl ein:

```
aws s3 cp \
    ${HOME}/ \
    s3://${BUCKET_NAME} \
    --recursive \
    [--exclude .cache/\*] // Optional
```

Schritt 7: Starten Sie eine Shell-Sitzung neu

> **Note**
>
> Als Sicherheitsmaßnahme wird die Sitzung automatisch beendet, wenn Sie über einen längeren Zeitraum nicht mit der Tastatur oder dem Zeiger mit der Shell interagieren. Sitzungen mit langer Laufzeit werden ebenfalls automatisch beendet. Weitere Informationen finden Sie unter Shell-Sitzungen.

1. Um eine Shell-Sitzung neu zu starten, wählen Sie Aktionen, Neustart AWS CloudShell.

Sie werden benachrichtigt, dass beim Neustart alle aktiven Sitzungen in der aktuellen AWS-Region Sitzung AWS CloudShell beendet werden.

2. Wählen Sie zur Bestätigung „Neu starten“.

   Eine Schnittstelle zeigt eine Meldung an, dass die CloudShell Rechenumgebung beendet wird. Nachdem die Umgebung gestoppt und neu gestartet wurde, können Sie in einer neuen Sitzung mit der Befehlszeile arbeiten.

   > **Note**
   >
   > In einigen Fällen kann es einige Minuten dauern, bis Ihre Umgebung neu gestartet wird.

Schritt 8: Löschen Sie das Home-Verzeichnis einer Shell-Sitzung

> **Note**
>
> Diese Option ist für VPC-Umgebungen nicht verfügbar. Wenn Sie eine VPC-Umgebung neu starten, wird ihr Home-Verzeichnis gelöscht.

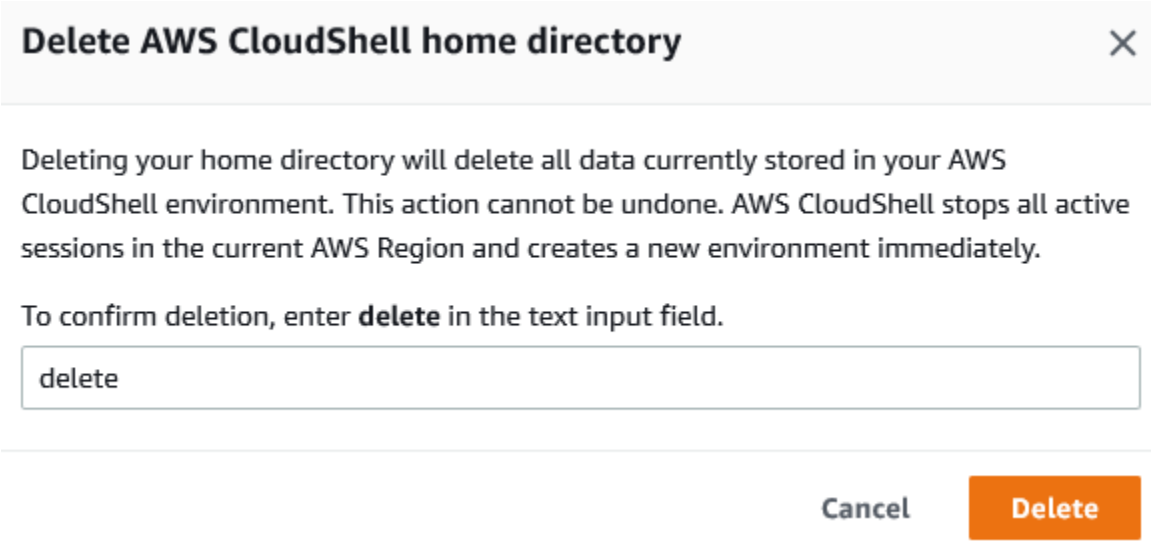
> **Warning**
>
> Das Löschen Ihres Home-Verzeichnisses ist eine unumkehrbare Aktion, bei der alle Daten, die in Ihrem Home-Verzeichnis gespeichert sind, dauerhaft gelöscht werden. In den folgenden Situationen sollten Sie diese Option jedoch in Betracht ziehen:
>
> - Sie haben eine Datei falsch geändert und können nicht auf die AWS CloudShell Rechenumgebung zugreifen. Wenn Sie Ihr Home-Verzeichnis löschen AWS CloudShell , werden die Standardeinstellungen wiederhergestellt.
> - Sie möchten alle Ihre Daten AWS CloudShell sofort entfernen. Wenn Sie die Nutzung AWS CloudShell in einer AWS Region beenden, wird der persistente Speicher am Ende des Aufbewahrungszeitraums automatisch gelöscht, sofern Sie nicht AWS CloudShell erneut in der Region starten.
>
> Wenn Sie Langzeitspeicher für Ihre Dateien benötigen, ziehen Sie bitte einen Service wie Amazon S3 oder in Betracht CodeCommit.

1. Um eine Shell-Sitzung zu löschen, wählen Sie Actions, Delete AWS CloudShell Home Directory.

   Sie werden darüber informiert, dass durch das Löschen des AWS CloudShell Home-Verzeichnisses alle Daten gelöscht werden, die derzeit in Ihrer AWS CloudShell Umgebung gespeichert sind.

   > **Note**
   >
   > Sie können diese Aktion nicht rückgängig machen.

2. Um den Löschvorgang zu bestätigen, geben Sie Löschen in das Texteingabefeld ein und wählen Sie dann Löschen.



   AWS CloudShell stoppt alle aktiven Sitzungen in der aktuellen Sitzung AWS-Region und erstellt sofort eine neue Umgebung.

   Manuelles Beenden von Shell-Sitzungen

   Mit der Befehlszeile können Sie eine Shell-Sitzung verlassen und sich mit dem `exit` Befehl abmelden. Sie können dann eine beliebige Taste drücken, um die Verbindung wiederherzustellen und die Nutzung AWS CloudShell fortzusetzen.

Schritt 9: Bearbeiten Sie den Code Ihrer Datei und führen Sie ihn über die Befehlszeile aus

Dieser Schritt zeigt, wie Sie den vorinstallierten Vim Editor verwenden, um mit einer Datei zu arbeiten. Anschließend führen Sie diese Datei als Programm von der Befehlszeile aus.

1. Geben Sie den folgenden Befehl ein, um die Datei zu bearbeiten, die Sie im vorherigen Schritt hochgeladen haben:

   ```
   vim add_prog.py
   ```

   Die Shell-Oberfläche wird aktualisiert und zeigt den Vim Editor an.

2. Um die Datei in zu bearbeitenVim, drücken Sie die I Taste. Bearbeiten Sie nun den Inhalt so, dass das Programm drei statt zwei Zahlen addiert.

   ```
   import sys
   x=int(sys.argv[1])
   y=int(sys.argv[2])
   z=int(sys.argv[3])
   sum=x+y+z
   print("The sum is",sum)
   ```

   > **Note**
   >
   > Wenn Sie den Text in den Editor einfügen und die Funktion Sicheres Einfügen aktiviert haben, wird eine Warnung angezeigt. Mehrzeiliger Text, der kopiert wird, kann bösartige Skripts enthalten. Mit der Funktion „Sicheres Einfügen“ können Sie den vollständigen Text überprüfen, bevor er eingefügt wird. Wenn Sie davon überzeugt sind, dass der Text sicher ist, wählen Sie Einfügen.

3. Nachdem Sie das Programm bearbeitet haben, drücken Sie, Esc um in den Vim Befehlsmodus zu gelangen. Geben Sie dann den `:wq` Befehl ein, um die Datei zu speichern und den Editor zu beenden.

> **Note**
>
> Wenn Sie mit dem Vim Befehlsmodus noch nicht vertraut sind, kann es zunächst schwierig sein, zwischen Befehlsmodus und Einfügemodus zu wechseln. Der Befehlsmodus wird beim Speichern von Dateien und beim Beenden der Anwendung verwendet. Der Einfügemodus wird beim Einfügen von neuem Text verwendet. Um in den Einfügemodus zu wechselnI, drücken Sie und, um in den Befehlsmodus zu wechseln, drücken SieEsc. Weitere Informationen zu Vim und anderen Tools, die in verfügbar sind AWS CloudShell, finden Sie unterEntwicklungstools und Shell-Dienstprogramme.

4. Führen Sie auf der Hauptbefehlszeilenschnittstelle das folgende Programm aus und geben Sie drei Zahlen für die Eingabe ein. Die Syntax ist wie folgt.

   ```
   python3 add_prog.py 4 5 6
   ```

   In der Befehlszeile wird die Programmausgabe angezeigt:`The sum is 15`.

Schritt 10: Verwenden Sie AWS CLI , um die Datei als Objekt in einem Amazon S3 S3-Bucket hinzuzufügen

In diesem Schritt erstellen Sie einen Amazon S3 S3-Bucket und verwenden dann die PutObjectMethode, um Ihre Codedatei als Objekt zu diesem Bucket hinzuzufügen.

> **Note**
>
> In den meisten Fällen können Sie einen Service verwenden, CodeCommit um beispielsweise eine Softwaredatei in ein versionskontrolliertes Repository zu übertragen. Dieses Tutorial zeigt, wie Sie AWS CLI in verwenden können AWS CloudShell , um mit anderen AWS-Services zu interagieren. Mit dieser Methode müssen Sie keine zusätzlichen Ressourcen herunterladen oder installieren. Da Sie außerdem bereits in der Shell authentifiziert sind, müssen Sie vor dem Tätigen von Anrufen keine Anmeldeinformationen konfigurieren.

1. Geben Sie den folgenden Befehl ein AWS-Region, um einen Bucket in einem bestimmten Bucket zu erstellen:

```
aws s3api create-bucket --bucket insert-unique-bucket-name-here --region us-east-1
```

> **Note**
>
> Wenn Sie einen Bucket außerhalb der `us-east-1` Region erstellen, fügen Sie ihn `create-bucket-configuration` mit dem `LocationConstraint` Parameter hinzu, um die Region anzugeben. Es folgt ein Beispiel für die Syntax.
>
> ```
> $ aws s3api create-bucket --bucket my-bucket --region eu-west-1 --create-
> bucket-configuration LocationConstraint=eu-west-1
> ```

Wenn der Aufruf erfolgreich ist, zeigt die Befehlszeile eine Antwort des Dienstes an, die der folgenden Ausgabe ähnelt.

```
{
    "Location": "/insert-unique-bucket-name-here"
}
```

> **Note**
>
> Wenn Sie sich nicht an die Regeln für die Benennung von Buckets halten, wird der folgende Fehler angezeigt: Beim Aufrufen der CreateBucket Operation ist ein Fehler aufgetreten (InvalidBucketName): Der angegebene Bucket ist nicht gültig.

2. Um eine Datei hochzuladen und die Datei als Objekt zu dem Bucket hinzuzufügen, den Sie gerade erstellt haben, rufen Sie die PutObject Methode auf.

```
aws s3api put-object --bucket insert-unique-bucket-name-here --key add_prog --body
 add_prog.py
```

Nachdem das Objekt in den Amazon S3 S3-Bucket hochgeladen wurde, zeigt die Befehlszeile eine Antwort des Service an, die der folgenden Ausgabe ähnelt:

```
{"ETag": "\"ab123c1:w:wad4a567d8bfd9a1234ebeea56\""}
```

Das `ETag` ist der Hash des Objekts, das gespeichert wurde. Sie können diesen Hash verwenden, um die Integrität des auf Amazon S3 hochgeladenen Objekts zu überprüfen.

Verwandte Themen

- Zusammenarbeit mitAWS Diensten inAWS CloudShell
- Tutorial: Kopieren mehrerer Dateien zwischen Ihrem lokalen Computer undAWS CloudShell
- Tutorial: Verwendung CodeCommit inAWS CloudShell
- Arbeiten mit AWS CloudShell
- Anpassen IhresAWS CloudShellErfahrung

AWS CloudShell-Anleitungen

Die folgenden Tutorials ermöglichen es Ihnen, verschiedene Funktionen und Integrationen bei der Verwendung AWS CloudShell zu experimentieren und zu testen.

Themen

Tutorial: Kopieren mehrerer Dateien zwischen Ihrem lokalen Computer undAWS CloudShell

Mithilfe der CloudShell Schnittstelle können Sie eine einzelne Datei gleichzeitig zwischen Ihrem lokalen Computer und der Shell-Umgebung hochladen oder herunterladen. Verwenden Sie eine der folgenden Optionen, um mehrere Dateien gleichzeitig zwischen CloudShell und Ihrem lokalen Computer zu kopieren:

- Amazon S3: Verwenden Sie S3-Buckets als Vermittler beim Kopieren von Dateien zwischen Ihrem lokalen Computer und CloudShell.
- Zip-Dateien: Komprimieren Sie mehrere Dateien in einem einzigen ZIP-Ordner, der über die CloudShell Benutzeroberfläche hoch- oder heruntergeladen werden kann.

> **Note**
>
> Da es CloudShell keinen eingehenden Internetverkehr zulässt, ist es derzeit nicht möglich, Befehle wie `scp` oder `rsync` das Kopieren mehrerer Dateien zwischen lokalen Computern und der CloudShell Computerumgebung zu verwenden.

Hochladen und Herunterladen mehrerer Dateien mit Amazon S3

Voraussetzungen

Um mit Buckets und Objekten arbeiten zu können, benötigen Sie eine IAM-Richtlinie, die Berechtigungen zur Ausführung der folgenden Amazon S3 S3-API-Aktionen gewährt:

- `s3:CreateBucket`
- `s3:PutObject`
- `s3:GetObject`

Eine vollständige Liste der Amazon S3 S3-Aktionen finden Sie unter Aktionen in der Amazon Simple Storage Service-API-Referenz.

Laden Sie mehrere Dateien hoch, um Amazon S3 zuAWS CloudShell verwenden

1. Erstellen Sie in einen S3-BucketAWS CloudShell, indem Sie den folgenden`s3` Befehl ausführen:

   ```
   aws s3api create-bucket --bucket your-bucket-name --region us-east-1
   ```

   Wenn der Aufruf erfolgreich ist, zeigt die Befehlszeile eine Antwort des S3-Dienstes an:

   ```
   {
       "Location": "/your-bucket-name"
   }
   ```

2. Laden Sie die Dateien in ein Verzeichnis von Ihrem lokalen Computer in den Bucket hoch. Wählen Sie eine der folgenden Optionen, um Dateien hochzuladen:

   - AWS Management Console: Wird verwendet drag-and-drop , um Dateien und Ordner in einen Bucket hochzuladen.
   - AWS CLI: Wenn die Version des Tools auf Ihrem lokalen Computer installiert ist, verwenden Sie die Befehlszeile, um Dateien und Ordner in den Bucket hochzuladen.

   Using the console

   - Öffnen Sie die Amazon S3 S3-Konsole unter https://s3.console.aws.amazon.com/s3/.

(Wenn Sie die Konsole verwendenAWS CloudShell, sollten Sie bereits bei der Konsole angemeldet sein.)

- Wählen Sie im linken Navigationsbereich Buckets aus und wählen Sie dann den Namen des Buckets aus, in den Ihre Ordner oder Dateien hochgeladen werden sollen. Sie können auch einen Bucket Ihrer Wahl erstellen, indem Sie „Bucket erstellen“ wählen.
- Wählen Sie Upload, um die Dateien und Ordner auszuwählen, die Sie hochladen möchten. Ziehen Sie dann Ihre ausgewählten Dateien und Ordner in das Konsolenfenster, das die Objekte im Ziel-Bucket auflistet, oder wählen Sie Dateien hinzufügen oder Ordner hinzufügen.

  Die von Ihnen ausgewählten Dateien werden auf der Upload-Seite aufgeführt.
- Markieren Sie die Kontrollkästchen, um die Dateien anzugeben, die hinzugefügt werden sollen.
- Um die ausgewählten Dateien zum Bucket hinzuzufügen, wählen Sie Upload.

> **Note**
>
> Informationen zu allen Konfigurationsoptionen bei der Verwendung der Konsole finden Sie unter Wie lade ich Dateien und Ordner in einen S3 Bucket hoch? im Amazon Simple Storage Service-Benutzerhandbuch.

Using AWS CLI

> **Note**
>
> Für diese Option müssen Sie dasAWS CLI Tool auf Ihrem lokalen Computer installiert haben und Ihre Anmeldeinformationen für Aufrufe vonAWS Diensten konfiguriert haben. Weitere Informationen finden Sie im AWS Command Line Interface-Benutzerhandbuch.

- Starten Sie dasAWS CLI Tool und führen Sie den folgenden`aws s3` Befehl aus, um den angegebenen Bucket mit dem Inhalt des aktuellen Verzeichnisses auf Ihrem lokalen Computer zu synchronisieren:

```
aws s3 sync folder-path s3://your-bucket-name
```

Wenn die Synchronisierung erfolgreich ist, werden Upload-Nachrichten für jedes Objekt angezeigt, das dem Bucket hinzugefügt wurde.

3. Kehren Sie zur CloudShell Befehlszeile zurück und geben Sie den folgenden Befehl ein, um das Verzeichnis in der Shell-Umgebung mit dem Inhalt des S3-Buckets zu synchronisieren:

```
aws s3 sync  s3://your-bucket-name folder-path
```

> **Note**
>
> Sie können dem`sync` Befehl auch`--include "<value>"` Parameter`--exclude "<value>"` und hinzufügen, um einen Musterabgleich durchzuführen, um eine bestimmte Datei oder ein bestimmtes Objekt entweder auszuschließen oder einzuschließen.
> Weitere Informationen finden Sie in der AWS CLIBefehlsreferenz unter Verwendung von Ausschluss- und Einschlussfiltern.

Wenn die Synchronisierung erfolgreich ist, werden Download-Meldungen für jede Datei angezeigt, die aus dem Bucket in das Verzeichnis heruntergeladen wurde.

> **Note**
>
> Mit dem Befehl sync werden nur neue und aktualisierte Dateien rekursiv aus dem Quellverzeichnis in das Ziel kopiert.

Laden Sie mehrere DateienAWS CloudShell mit Amazon S3 herunter

1. Geben Sie über dieAWS CloudShell Befehlszeile den folgenden`aws s3` Befehl ein, um einen S3-Bucket mit dem Inhalt des aktuellen Verzeichnisses in der Shell-Umgebung zu synchronisieren:

```
aws s3 sync folder-path s3://your-bucket-name
```

> **Note**
>
> Sie können dem`sync` Befehl auch`--include "<value>"` Parameter`--exclude "<value>"` und hinzufügen, um einen Musterabgleich durchzuführen, um eine bestimmte Datei oder ein bestimmtes Objekt entweder auszuschließen oder einzuschließen.
> Weitere Informationen finden Sie in der AWS CLIBefehlsreferenz unter Verwendung von Ausschluss- und Einschlussfiltern.

Wenn die Synchronisierung erfolgreich ist, werden Upload-Nachrichten für jedes Objekt angezeigt, das dem Bucket hinzugefügt wurde.

2. Laden Sie den Inhalt des Buckets auf Ihren lokalen Computer herunter. Da die Amazon S3 S3-Konsole das Herunterladen mehrerer Objekte nicht unterstützt, müssen Sie dasAWS CLI Tool verwenden, das auf Ihrem lokalen Computer installiert ist.

   Führen Sie in der Befehlszeile desAWS CLI Tools den folgenden Befehl aus.

   ```
   aws s3 sync s3://your-bucket-name folder-path
   ```

   Wenn die Synchronisierung erfolgreich ist, zeigt die Befehlszeile eine Download-Meldung für jede Datei an, die im Zielverzeichnis aktualisiert oder hinzugefügt wurde.

   > **Note**
   >
   > Für diese Option müssen Sie dasAWS CLI Tool auf Ihrem lokalen Computer installiert haben und Ihre Anmeldeinformationen für Aufrufe vonAWS Diensten konfiguriert haben. Weitere Informationen finden Sie im AWS Command Line Interface-Benutzerhandbuch.

Hochladen und Herunterladen mehrerer Dateien mithilfe von Zip-Ordnern

Mit den Dienstprogrammen zum Komprimieren und Entpacken können Sie mehrere Dateien in einem Archiv komprimieren, das als eine einzige Datei behandelt werden kann. Die Dienstprogramme sind in der CloudShell Computerumgebung vorinstalliert.

Weitere Informationen zu vorinstallierten Tools finden Sie unterEntwicklungstools und Shell-Dienstprogramme.

Laden Sie mehrere Dateien hoch, umAWS CloudShell komprimierte Ordner zu verwenden

1. Fügen Sie auf Ihrem lokalen Computer die hochzuladenden Dateien in einen ZIP-Ordner hinzu.
2. Starten CloudShell Sie und wählen Sie dann Aktionen, Datei hochladen.
3. Wählen Sie im Dialogfeld Datei hochladen die Option Datei auswählen und wählen Sie dann den ZIP-Ordner aus, den Sie gerade erstellt haben.
4. Wählen Sie im Dialogfeld Datei hochladen die Option Hochladen, um die ausgewählte Datei zur Shell-Umgebung hinzuzufügen.
5. Führen Sie in der CloudShell Befehlszeile den folgenden Befehl aus, um den Inhalt des ZIP-Archivs in ein bestimmtes Verzeichnis zu entpacken:

   ```
   unzip zipped-files.zip -d my-unzipped-folder
   ```

Laden Sie mehrere DateienAWS CloudShell mithilfe von Zip-Ordnern herunter

1. Führen Sie in der CloudShell Befehlszeile den folgenden Befehl aus, um alle Dateien im aktuellen Verzeichnis zu einem komprimierten Ordner hinzuzufügen:

   ```
   zip -r zipped-archive.zip *
   ```

2. Wählen Sie Aktionen, Datei herunterladen.
3. Geben Sie im Dialogfeld Datei herunterladen den Pfad für den komprimierten Ordner ein (`/home/cloudshell-user/zip-folder/zipped-archive.zip`z. B.) und wählen Sie dann Herunterladen.

   Wenn der Pfad korrekt ist, bietet ein Browser-Dialog die Möglichkeit, den komprimierten Ordner zu öffnen oder auf Ihrem lokalen Computer zu speichern.
4. Auf Ihrem lokalen Computer können Sie jetzt den Inhalt des heruntergeladenen Zip-Ordners entpacken.

Tutorial: Verwendung CodeCommit inAWS CloudShell

CodeCommit ist ein sicherer, hochgradig skalierbarer und verwalteter Service für Quellüberwachung, der private Git-Repositorys hostet. MitAWS CloudShell können Sie mit CodeCommit dem git-remote-codecommitDienstprogramm in der Befehlszeile arbeiten. Dieses Dienstprogramm ist in derAWS CloudShell Computerumgebung vorinstalliert und bietet eine einfache Methode zum Push und Abrufen von Code aus CodeCommit Repositorys. Dieses Tool tut dies, indem es Git erweitert. Weitere Informationen finden Sie im AWS CodeCommit-Benutzerhandbuch.

In diesem Tutorial wird beschrieben, wie Sie ein CodeCommit Repository erstellen und es in IhreAWS CloudShell Computerumgebung klonen. Sie lernen auch, wie Sie eine Datei bereitstellen und in Ihr geklontes Repository übertragen, bevor Sie sie in das Remote-Repository übertragen, das in derAWS Cloud verwaltet wird.

Voraussetzungen

Informationen zu den Berechtigungen, die ein IAM-Benutzer für die Verwendung benötigtAWS CloudShell, finden Sie im Abschnitt Voraussetzungen im Tutorial Erste Schritte. Sie benötigen außerdem IAM-Berechtigungen, um damit zu arbeiten CodeCommit.

Stellen Sie außerdem sicher, dass Sie vor dem Start Folgendes haben:

- Ein grundlegendes Verständnis von Git-Befehlen und Versionskontrollkonzepten
- Eine Datei im Home-Verzeichnis Ihrer Shell, die in die lokalen und externen Repositorys übertragen werden kann. In diesem Tutorial wird es als bezeichnet`my-git-file`.

Schritt 1: Erstellen und Klonen von CodeCommit Repositorys

1. Geben Sie in der CloudShell Befehlszeilenschnittstelle den folgenden`codecommit` Befehl ein, um ein CodeCommit Repository namens zu erstellen`MyDemoRepo`.

   ```
   aws codecommit create-repository --repository-name MyDemoRepo --repository-
   description "My demonstration repository"
   ```

   Wenn das Repository erfolgreich erstellt wurde, zeigt die Befehlszeile die Antwort des Dienstes an.

   ```
   {
   ```

```
    "repositoryMetadata": {
        "accountId": "111122223333",
        "repositoryId": "0dcd29a8-941a-1111-1111-11111111111a",
        "repositoryName": "MyDemoRepo",
        "repositoryDescription": "My demonstration repository",
        "lastModifiedDate": "2020-11-23T20:38:23.068000+00:00",
        "creationDate": "2020-11-23T20:38:23.068000+00:00",
        "cloneUrlHttp": "https://git-codecommit.eu-west-1.amazonaws.com/v1/repos/
MyDemoRepo",
        "cloneUrlSsh": "ssh://git-codecommit.eu-west-1.amazonaws.com/v1/repos/
MyDemoRepo",
        "Arn": "arn:aws:codecommit:eu-west-1:111111111111:MyDemoRepo"
     }
 )
```

2. Erstellen Sie über die Befehlszeile ein neues Verzeichnis für Ihr lokales Repository und machen Sie es zum Arbeitsverzeichnis.

```
mkdir my-shell-repo
cd my-shell-repo
```

3. Um das Remote-Repository zu klonen, verwenden Sie den`git clone` Befehl. (Verwenden Sie bei git-remote-codecommitder Arbeit den URL-Stil HTTPS (GRC).)

```
git clone codecommit::eu-west-1://MyDemoRepo
```

   Wenn das Repository erfolgreich geklont wurde, zeigt die Befehlszeile die Antwort des Dienstes an.

```
Cloning into 'MyDemoRepo'...
warning: You appear to have cloned an empty repository.
```

4. Verwenden Sie den`cd` Befehl, um zum geklonten Repository zu navigieren.

```
cd MyDemoRepo
```

Schritt 2: Stage und Commit einer Datei, bevor du sie in dein CodeCommit Repository verschiebst

1. Fügen Sie dem`MyDemoRepo` Ordner eine aufgerufene Datei`my-git-file` hinzu, indem Sie entweder einen Vim-Editor oder die Datei-Upload-Funktion von verwendenAWS CloudShell. Weitere Informationen zur Verwendung von beiden finden Sie im Tutorial Erste Schritte.
2. Um Ihre Datei im Repository zu speichern, führen Sie den`add` Befehl git aus.

   ```
   git add my-git-file
   ```

3. Führen Sie den`status` Befehl git aus, um zu überprüfen, ob die Datei bereitgestellt wurde und zum Commit bereit ist.

   ```
   git status
   ```

   `my-git-file`wird als neue Datei aufgeführt und in grünem Text angezeigt, was darauf hinweist, dass sie zum Commit bereit ist.
4. Übertragen Sie diese Version der Staging-Datei in das Repository.

   ```
   git commit -m "first commit to repo"
   ```

   > **Note**
   >
   > Wenn Sie nach Konfigurationsinformationen gefragt werden, um den Commit abzuschließen, verwenden Sie das folgende Format.
   >
   > ```
   > $ git config --global user.name "Jane Doe"
   > $ git config --global user.email janedoe@example.com
   > ```

5. Um Ihr Remote-Repository mit den Änderungen in Ihrem lokalen Repository zu synchronisieren, übertragen Sie die Änderungen in den Upstream-Zweig.

   ```
   git push
   ```

Tutorial: Eine vorsignierte URL für Amazon S3 SS3-ObjekteAWS CloudShell

Dieses Tutorial zeigt Ihnen, wie eine vorsignierte URL eines Amazon SSSSSSSSS-SAmazon S3 S3-Objekt mit anderen Da Objektbesitzer beim Teilen ihre eigenen Sicherheitsanmeldeinformationen angeben, kann jeder, der die vorsignierte URL erhält, für eine begrenzte Zeit auf das Objekt zugreifen.

Voraussetzungen

- Ein IAM-Benutzer mit den in der AWSCloudShellFullAccessRichtlinie bereitgestellten Zugriffsberechtigungen.
- Die IAM-Berechtigungen, die zum Erstellen einer vorsignierten URL erforderlich sind, finden Sie im Amazon Simple Storage Service-Benutzerhandbuch unter Teilen eines Objekts für andere.

Schritt 1: Eine IAM-Rolle, um Zugriff auf den Amazon-SS-SAmazon S3 Bucket

1. Rufen Sie den`get-caller-identity` Befehl von auf, um Ihre IAM-Details zu erhalten, die geteilt werden könnenAWS CloudShell.

   ```
   aws sts get-caller-identity
   ```

   Wenn der Aufruf erfolgreich ist, zeigt die Befehlszeile eine Antwort ähnlich der folgenden an.

   ```
   {
       "Account": "123456789012",
       "UserId": "AROAXXOZUUOTTWDCVIDZ2:redirect_session",
       "Arn": "arn:aws:sts::531421766567:assumed-role/Feder08/redirect_session"
   }
   ```

2. Nehmen Sie die Benutzerinformationen, die Sie im vorherigen Schritt erhalten haben, und fügen Sie sie einerAWS CloudFormation Vorlage hinzu. Diese Vorlage Diese Rolle gewährt Ihrem Mitarbeiter die geringsten Rechte für die gemeinsam genutzten Ressourcen.

   ```
   Resources:
     CollaboratorRole:
   ```

```
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              AWS: "arn:aws:iam::531421766567:role/Feder08"
            Action: "sts:AssumeRole"
      Description: Role used by my collaborators
      MaxSessionDuration: 7200
  CollaboratorPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action:
              - 's3:*'
            Resource: 'arn:aws:s3:::<YOUR_BUCKET_FOR_FILE_TRANSFER>'
            Condition:
              StringEquals:
                s3:prefix:
                 - "myfolder/*"
      PolicyName: S3ReadSpecificFolder
      Roles:
        - !Ref CollaboratorRole
Outputs:
  CollaboratorRoleArn:
    Description: Arn for the Collaborator's Role
    Value: !GetAtt CollaboratorRole.Arn
```

3. Speichern Sie dieAWS CloudFormation Vorlage in einer Datei, die benannt ist`template.yaml`.
4. Verwenden Sie die Vorlage, um den Stack bereitzustellen und die IAM-Rolle zu erstellen, indem Sie den`deploy` Befehl aufrufen.

```
aws cloudformation deploy --template-file ./template.yaml --stack-name
 CollaboratorRole --capabilities CAPABILITY_IAM
```

Generieren

1. Verwenden Sie Ihren EditorAWS CloudShell und fügen Sie den folgenden Code hinzu. Dieser Code erstellt eine URL, die Verbundbenutzern direkten Zugriff auf die bietetAWS Management Console.

```
import urllib, json, sys
import requests
import boto3
import os

def main():
  sts_client = boto3.client('sts')
  assume_role_response = sts_client.assume_role(
      RoleArn=os.environ.get(ROLE_ARN),
      RoleSessionName="collaborator-session"
  )
  credentials = assume_role_response['Credentials']
  url_credentials = {}
  url_credentials['sessionId'] = credentials.get('AccessKeyId')
  url_credentials['sessionKey'] = credentials.get('SecretAccessKey')
  url_credentials['sessionToken'] = credentials.get('SessionToken')
  json_string_with_temp_credentials = json.dumps(url_credentials)
  print(f"json string {json_string_with_temp_credentials}")

  request_parameters = f"?
Action=getSigninToken&Session={urllib.parse.quote(json_string_with_temp_credentials)}"
  request_url = "https://signin.aws.amazon.com/federation" + request_parameters
  r = requests.get(request_url)
  signin_token = json.loads(r.text)
  request_parameters = "?Action=login"
  request_parameters += "&Issuer=Example.org"
  request_parameters += "&Destination=" + urllib.parse.quote("https://us-
west-2.console.aws.amazon.com/cloudshell")
  request_parameters += "&SigninToken=" + signin_token["SigninToken"]
  request_url = "https://signin.aws.amazon.com/federation" + request_parameters

  # Send final URL to stdout
  print (request_url)

if __name__ == "__main__":
  main()
```

2. Speichern Sie den Code in einer Datei namens`share.py`.
3. Das Folgende an der Befehlszeile, um den Amazon-Ressourcennamen (ARN) der IAM-Rolle (ARN) der IAM-Rolle versehen seinAWS CloudFormation. Benutze es dann imPython Skript, um temporäre Sicherheitsanmeldeinformationen zu erhalten.

```
ROLE_ARN=$(aws cloudformation describe-stacks --stack-name CollaboratorRole --query
 "Stacks[*].Outputs[?OutputKey=='CollaboratorRoleArn'].OutputValue" --output text)
 python3 ./share.py
```

   Das Skript gibt eine URL zurück, auf die ein Mitarbeiter klicken kann, um zu ihmAWS CloudShell zu gelangenAWS Management Console. Der Mitarbeiter hat für die nächsten 3.600 Sekunden (1 Stunde) die volle Kontrolle über den`myfolder/` Ordner im Amazon S3 S3-Bucket. Die Anmeldeinformationen laufen nach einer Stunde ab. Nach Ablauf dieser Zeit kann der Mitarbeiter nicht mehr auf den Bucket zugreifen.

Tutorial: Einen Docker-Container im Inneren erstellen AWS CloudShell und in ein Amazon ECR-Repository verschieben

Dieses Tutorial zeigt Ihnen, wie Sie einen Docker-Container definieren und erstellen AWS CloudShell und ihn in ein Amazon ECR-Repository übertragen.

Voraussetzungen

- Sie müssen über die erforderlichen Berechtigungen verfügen, um ein Amazon ECR-Repository zu erstellen und in dieses zu übertragen. Weitere Informationen zu Repositorys mit Amazon ECR finden Sie unter Private Amazon ECR-Repositorys im Amazon ECR-Benutzerhandbuch. Weitere Informationen zu den Berechtigungen, die für das Übertragen von Bildern mit Amazon ECR erforderlich sind, finden Sie unter Erforderliche IAM-Berechtigungen für das Übertragen eines Bilds im Amazon ECR-Benutzerhandbuch.

Ablauf des Tutorials

Das folgende Tutorial beschreibt, wie Sie die CloudShell Schnittstelle verwenden, um einen Docker-Container zu erstellen und ihn in ein Amazon ECR-Repository zu übertragen.

1. Erstellen Sie einen neuen Ordner in Ihrem Home-Verzeichnis.

```
mkdir ~/docker-cli-tutorial
```

2. Navigieren Sie zu dem Ordner, den Sie erstellt haben.

```
cd ~/docker-cli-tutorial
```

3. Erstellen Sie ein leeres Dockerfile.

```
touch Dockerfile
```

4. Öffnen Sie die Datei beispielsweise `nano Dockerfile` mit einem Texteditor und fügen Sie den folgenden Inhalt ein.

```
# Dockerfile

# Base this container on the latest Amazon Linux version
FROM public.ecr.aws/amazonlinux/amazonlinux:latest

# Install the cowsay binary
RUN dnf install --assumeyes cowsay

# Default entrypoint binary
ENTRYPOINT [ "cowsay" ]

# Default argument for the cowsay entrypoint
CMD [ "Hello, World!" ]
```

5. Das Dockerfile kann jetzt erstellt werden. Erstellen Sie den Container, indem Sie ihn ausführen. `docker build` Kennzeichnen Sie den Container mit einem easy-to-type Namen, der in future Befehlen verwendet werden kann.

```
docker build --tag test-container .
```

Stellen Sie sicher, dass Sie den letzten Punkt (`.`) angeben.

6. Sie können den Container jetzt testen, um zu überprüfen, ob er korrekt ausgeführt wird. AWS CloudShell

```
docker container run test-container
```

7. Da Sie nun über einen funktionierenden Docker-Container verfügen, müssen Sie ihn in ein Amazon ECR-Repository verschieben. Wenn Sie bereits über ein Amazon ECR-Repository verfügen, können Sie diesen Schritt überspringen.

   Führen Sie den folgenden Befehl aus, um ein Amazon ECR-Repository für dieses Tutorial zu erstellen.

   ```
   ECR_REPO_NAME=docker-tutorial-repo
   aws ecr create-repository --repository-name ${ECR_REPO_NAME}
   ```

8. Nachdem Sie das Amazon ECR-Repository erstellt haben, können Sie den Docker-Container dorthin verschieben.

   Führen Sie den folgenden Befehl aus, um die Amazon ECR-Anmeldeinformationen für Docker abzurufen.

   ```
   AWS_ACCOUNT_ID=$(aws sts get-caller-identity --query "Account" --output text)
   ECR_URL=${AWS_ACCOUNT_ID}.dkr.ecr.${AWS_REGION}.amazonaws.com
   aws ecr get-login-password | docker login --username AWS --password-stdin
    ${ECR_URL}
   ```

9. Taggen Sie das Bild mit dem Amazon ECR-Ziel-Repository und übertragen Sie es dann in dieses Repository.

   ```
   docker tag test-container ${ECR_URL}/${ECR_REPO_NAME}
   docker push ${ECR_URL}/${ECR_REPO_NAME}
   ```

   Wenn Sie beim Durcharbeiten dieses Tutorials auf Fehler oder Probleme stoßen, finden Sie im Abschnitt zur Fehlerbehebung in diesem Handbuch Hilfe.

Bereinigen

Sie haben Ihren Docker-Container jetzt erfolgreich in Ihrem Amazon ECR-Repository bereitgestellt. Führen Sie den folgenden Befehl aus, um die Dateien, die Sie in diesem Tutorial erstellt haben, aus Ihrer AWS CloudShell Umgebung zu entfernen.

- ```
  cd ~
  ```
  ```

```
rm -rf ~/docker-cli-tutorial
```

- Löschen Sie das Amazon ECR-Repository.

```
aws ecr delete-repository --force --repository-name ${ECR_REPO_NAME}
```

Tutorial: Bereitstellen einer Lambda-Funktion mit dem AWS CDK

Dieses Tutorial zeigt Ihnen, wie Sie mithilfe von eine Lambda-Funktion für Ihr Konto bereitstellen. AWS Cloud Development Kit (AWS CDK)

Voraussetzungen

- Starten Sie Ihr Konto für die Verwendung mit dem. AWS CDK Informationen zum Bootstrapping mit AWS CDK finden Sie unter Bootstrapping im v2 Developer Guide. AWS CDK Wenn Sie das Konto noch nicht gebootet haben, können Sie es ausführen. `cdk bootstrap` CloudShell

- Stellen Sie sicher, dass Sie über die entsprechenden Berechtigungen verfügen, um Ressourcen für Ihr Konto bereitzustellen. Administratorrechte werden empfohlen.

Ablauf des Tutorials

Das folgende Tutorial beschreibt, wie Sie eine auf einem Docker-Container basierende Lambda-Funktion mithilfe von bereitstellen. AWS CDK

1. Erstellen Sie einen neuen Ordner in Ihrem Home-Verzeichnis.

   ```
   mkdir ~/docker-cdk-tutorial
   ```

2. Navigieren Sie zu dem Ordner, den Sie erstellt haben.

   ```
   cd ~/docker-cdk-tutorial
   ```

3. Installieren Sie die AWS CDK Abhängigkeiten lokal.

   ```
   npm install aws-cdk aws-cdk-lib
   ```

4. Erstellen Sie ein AWS CDK Skelettprojekt in dem Ordner, den Sie erstellt haben.

```
touch cdk.json
mkdir lib
touch lib/docker-tutorial.js lib/Dockerfile lib/hello.js
```

5. Öffnen Sie die Datei `nano cdk.json` beispielsweise mit einem Texteditor und fügen Sie den folgenden Inhalt ein.

```
{
  "app": "node lib/docker-tutorial.js"
}
```

6. Öffnen Sie die `lib/docker-tutorial.js` Datei und fügen Sie den folgenden Inhalt ein.

```
// this file defines the CDK constructs we want to deploy

const { App, Stack } = require('aws-cdk-lib');
const { DockerImageFunction, DockerImageCode } = require('aws-cdk-lib/aws-lambda');
const path = require('path');

// create an application
const app = new App();

// define stack
class DockerTutorialStack extends Stack {
  constructor(scope, id, props) {
    super(scope, id, props);

    // define lambda that uses a Docker container
    const dockerfileDir = path.join(__dirname);
    new DockerImageFunction(this, 'DockerTutorialFunction', {
      code: DockerImageCode.fromImageAsset(dockerfileDir),
      functionName: 'DockerTutorialFunction',
    });
  }
}

// instantiate stack
new DockerTutorialStack(app, 'DockerTutorialStack');
```

7. Öffnen Sie die `lib/Dockerfile` und fügen Sie den folgenden Inhalt ein.

```
# Use a NodeJS 20.x runtime
FROM public.ecr.aws/lambda/nodejs:20

# Copy the function code to the LAMBDA_TASK_ROOT directory
# This environment variable is provided by the lambda base image
COPY hello.js ${LAMBDA_TASK_ROOT}

# Set the CMD to the function handler
CMD [ "hello.handler" ]
```

8. Öffnen Sie die `lib/hello.js` Datei und fügen Sie den folgenden Inhalt ein.

```
// define the handler
exports.handler = async (event) => {
  // simply return a friendly success response
  const response = {
    statusCode: 200,
    body: JSON.stringify('Hello, World!'),
  };
  return response;
};
```

9. Verwenden Sie die AWS CDK CLI, um das Projekt zu synthetisieren und die Ressourcen bereitzustellen. Sie müssen Ihr Konto booten.

```
npx cdk synth
npx cdk deploy --require-approval never
```

10. Rufen Sie die Lambda-Funktion auf, um dies zu bestätigen und zu verifizieren.

```
aws lambda invoke --function-name DockerTutorialFunction out.json
jq . out.json
```

Sie haben jetzt erfolgreich eine Container-basierte Docker-Lambda-Funktion mit dem bereitgestellt. AWS CDK Weitere Informationen dazu finden Sie im v2 AWS CDK Developer Guide. AWS CDK Wenn Sie beim Durcharbeiten dieses Tutorials auf Fehler oder Probleme stoßen, finden Sie im Abschnitt zur Fehlerbehebung in diesem Handbuch Hilfe.

Bereinigen

Sie haben jetzt erfolgreich eine Container-basierte Docker-Lambda-Funktion mit dem bereitgestellt. AWS CDK Führen Sie innerhalb des AWS CDK Projekts den folgenden Befehl aus, um die zugehörigen Ressourcen zu löschen. Sie werden aufgefordert, den Löschvorgang zu bestätigen.

- ```
  npx cdk destroy DockerTutorialStack
  ```
- Führen Sie den folgenden Befehl aus, um die Dateien und Ressourcen, die Sie in diesem Tutorial erstellt haben, aus Ihrer AWS CloudShell Umgebung zu entfernen.

  ```
  cd ~
  rm -rf ~/docker-cli-tutorial
  ```
  ```

Arbeiten mit AWS CloudShell

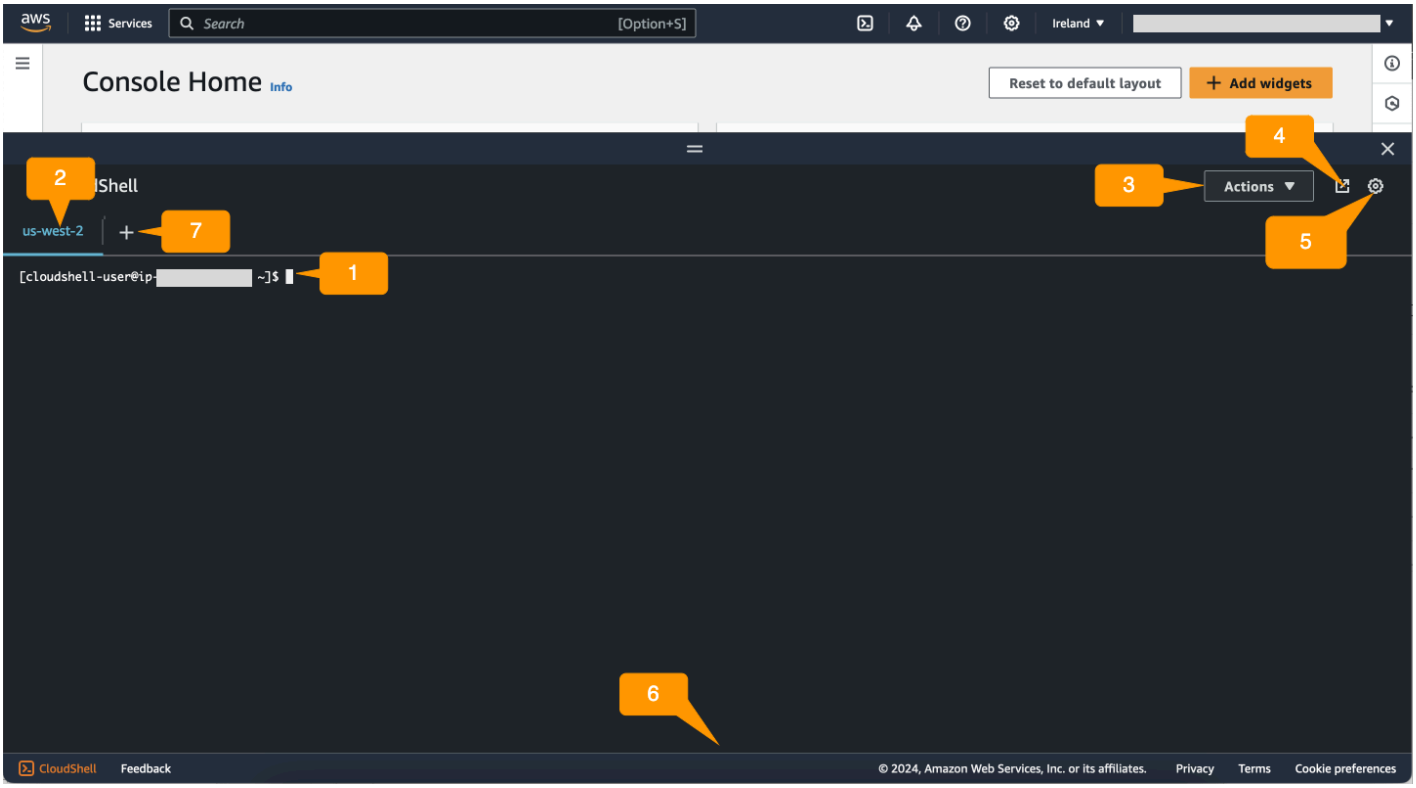
In diesem Abschnitt wird beschrieben, wie Sie mit unterstützten Anwendungen interagieren AWS CloudShell und bestimmte Aktionen ausführen können.

Themen

In der Benutzeroberfläche navigieren AWS CloudShell

Sie können vom AWS Management Console und Console Toolbar aus durch die Funktionen der CloudShell Benutzeroberfläche navigieren.

Der folgende Screenshot zeigt mehrere wichtige Funktionen der AWS CloudShell Benutzeroberfläche.



1. AWS CloudShell Befehlszeilenschnittstelle, mit der Sie Befehle mithilfe Ihrer bevorzugten Shell ausführen. Der aktuelle Shell-Typ wird in der Befehlszeile angezeigt.
2. Die Terminal-Registerkarte, die angibt, AWS-Region wo gerade ausgeführt AWS CloudShell wird.
3. Das Aktionsmenü, das Optionen zum Ändern des Bildschirmlayouts, zum Herunterladen und Hochladen von Dateien, zum Neustarten und Löschen Ihres AWS CloudShellAWS CloudShell Home-Verzeichnisses enthält.

   > **Note**
   >
   > Die Download-Option ist nicht verfügbar, wenn Sie CloudShell auf dem starten. Console Toolbar

4. Die Registerkarte In neuem Browser öffnen, auf der Sie im Vollbildmodus auf Ihre CloudShell Sitzung zugreifen können.
5. Die Option „Einstellungen“, mit der Sie Ihr Shell-Erlebnis anpassen können.
6. Die untere Leiste bietet folgende Optionen für:
   - Starten Sie CloudShell über das CloudShellSymbol.
   - Geben Sie Feedback über das Feedback-Symbol. Wählen Sie die Art des Feedbacks aus, das Sie einreichen möchten, fügen Sie Ihre Kommentare hinzu und wählen Sie dann Senden aus.
     - Um Feedback einzureichen CloudShell, wählen Sie eine der folgenden Optionen:
       - Starten Sie CloudShell von der Konsole aus und wählen Sie Feedback aus. Fügen Sie Ihre Kommentare hinzu und wählen Sie dann Senden aus.
       - Wählen Sie CloudShellunten links in der Konsole Feedback aus und wählen Sie dann In neuem Browser-Tab öffnen aus. Console Toolbar Fügen Sie Ihre Kommentare hinzu und wählen Sie dann Absenden.

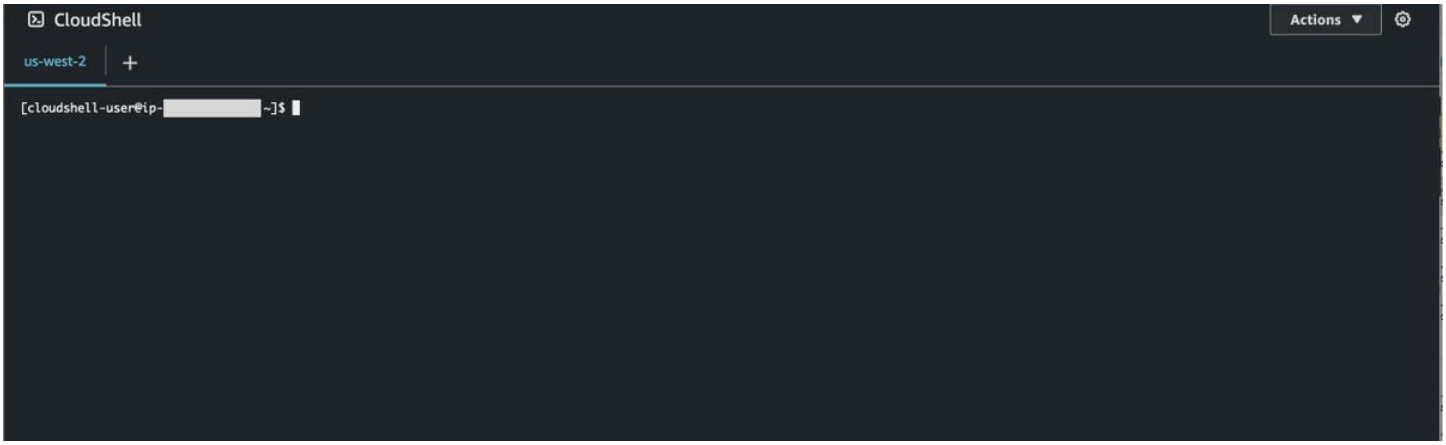
     > **Note**
     >
     > Die Feedback-Option ist nicht verfügbar, wenn Sie CloudShell am startenConsole Toolbar.

   - Erfahre mehr über unsere Datenschutzrichtlinien und Nutzungsbedingungen und passe deine Cookie-Präferenzen an.

7. Das Pluszeichen ist ein Dropdownmenü, das Optionen zum Erstellen, Neustarten und Löschen von Umgebungen enthält.

Arbeitet in AWS-Regionen

Der aktuelle AWS-Region Modus, in dem Sie gerade arbeiten, wird als Tab angezeigt.



Sie können eine Region auswählen, in der Sie arbeiten AWS-Region möchten, indem Sie mit der Regionsauswahl eine bestimmte Region auswählen. Nachdem Sie die Regionen geändert haben, wird die Benutzeroberfläche aktualisiert, wenn Ihre Shell-Sitzung eine Verbindung zu einer anderen Computerumgebung herstellt, die in der ausgewählten Region ausgeführt wird.

Important

- Sie können jeweils AWS-Region bis zu 1 GB persistenten Speicher verwenden. Persistenter Speicher wird in Ihrem Home-Verzeichnis (`$HOME`) gespeichert. Das bedeutet, dass sich alle persönlichen Dateien, Verzeichnisse, Programme oder Skripts, die in Ihrem Home-Verzeichnis gespeichert sind, alle in einem Verzeichnis befinden AWS-Region. Außerdem unterscheiden sie sich von denen, die sich im Home-Verzeichnis befinden und in einer anderen Region gespeichert sind.

  Die langfristige Aufbewahrung von Dateien im persistenten Speicher wird ebenfalls auf regionaler Basis verwaltet. Weitere Informationen finden Sie unter Persistenter Speicher.
- Persistenter Speicher ist für AWS CloudShell VPC-Umgebungen nicht verfügbar.

Geben Sie Ihren Standard für AWS-Region an AWS CLI

Sie können Umgebungsvariablen verwenden, um Konfigurationsoptionen und Anmeldeinformationen anzugeben, die für den AWS-Services Zugriff erforderlich sind AWS CLI. Die Umgebungsvariable, die den Standard AWS-Region für Ihre Shell-Sitzung angibt, wird entweder gesetzt, wenn Sie AWS CloudShell von einer bestimmten Region aus starten AWS Management Console oder wenn Sie eine Option in der Regionsauswahl auswählen.

Umgebungsvariablen haben Vorrang vor AWS CLI Anmeldeinformationsdateien, die von aktualisiert werden. `aws configure` Sie können den `aws configure` Befehl zum Ändern der Region, die durch die Umgebungsvariable angegeben ist, also nicht ausführen. Um stattdessen die Standardregion für AWS CLI Befehle zu ändern, weisen Sie der `AWS_REGION` Umgebungsvariablen einen Wert zu. Ersetzen Sie es in den folgenden Beispielen `us-east-1` durch die Region, in der Sie sich befinden.

Bash or Zsh

```
$ export AWS_REGION=us-east-1
```

Wenn Sie die Umgebungsvariable festlegen, ändert sich der Wert, der verwendet wird, bis Sie entweder Ihre Shell-Sitzung beenden oder die Variable auf einen anderen Wert setzen. Sie können Variablen im Startskript Ihrer Shell festlegen, um die Variablen für future Sitzungen persistent zu machen.

PowerShell

```
PS C:\> $Env:AWS_REGION="us-east-1"
```

Wenn Sie an der PowerShell Eingabeaufforderung eine Umgebungsvariable festlegen, speichert die Umgebungsvariable den Wert nur für die Dauer der aktuellen Sitzung. Alternativ können Sie die Variable für alle future PowerShell Sitzungen festlegen, indem Sie die Variable zu Ihrem PowerShell Profil hinzufügen. Weitere Informationen zum Speichern von Umgebungsvariablen finden Sie in der PowerShell Dokumentation.

Um zu bestätigen, dass Sie die Standardregion geändert haben, führen Sie den `aws configure list` Befehl aus, um die aktuellen AWS CLI Konfigurationsdaten anzuzeigen.

> **Note**
>
> Bei bestimmten AWS CLI Befehlen können Sie die Standardregion mithilfe der Befehlszeilenoption überschreiben`--region`. Weitere Informationen finden Sie im AWS Command Line Interface Benutzerhandbuch unter Befehlszeilenoptionen.

Arbeiten mit Dateien und Speicher

Über AWS CloudShell die Benutzeroberfläche können Sie Dateien in die Shell-Umgebung hochladen und Dateien aus der Shell-Umgebung herunterladen. Weitere Informationen zum Herunterladen und Hochladen von Dateien finden Sie unter Erste Schritte mit AWS CloudShell.

Um sicherzustellen, dass alle von Ihnen hinzugefügten Dateien auch nach Ende der Sitzung verfügbar sind, sollten Sie den Unterschied zwischen persistentem und temporärem Speicher kennen.

- Dauerhafter Speicher: Sie verfügen jeweils über 1 GB persistenten Speicher AWS-Region. Persistenter Speicher befindet sich in Ihrem Home-Verzeichnis.
- Temporärer Speicher: Temporärer Speicher wird am Ende einer Sitzung wiederverwendet. Temporärer Speicher befindet sich in den Verzeichnissen, die sich außerhalb Ihres Home-Verzeichnisses befinden.

> **Important**
>
> Stellen Sie sicher, dass Sie Dateien, die Sie behalten und für future Shell-Sitzungen verwenden möchten, in Ihrem Home-Verzeichnis belassen. Nehmen wir beispielsweise an, Sie verschieben eine Datei aus Ihrem Home-Verzeichnis, indem Sie den `mv` Befehl ausführen. Diese Datei wird dann recycelt, wenn die aktuelle Shell-Sitzung endet.

Arbeiten mit Docker

AWS CloudShell unterstützt Docker vollständig ohne Installation oder Konfiguration. Sie können Docker-Container darin definieren, erstellen und ausführen. AWS CloudShell Sie können Docker-basierte Ressourcen wie Lambda-Funktionen, die auf Docker-Containern basieren, über das AWS CDK Toolkit bereitstellen sowie Docker-Container erstellen und diese über die Docker-CLI in Amazon

ECR-Repositorys übertragen. Detaillierte Schritte zur Ausführung dieser beiden Bereitstellungen finden Sie in den folgenden Tutorials:

- Tutorial: Bereitstellen einer Lambda-Funktion mit dem AWS CDK
- Tutorial: Einen Docker-Container im Inneren erstellen AWS CloudShell und in ein Amazon ECR-Repository verschieben

Es gibt bestimmte Einschränkungen und Einschränkungen bei der Verwendung von Docker mit: AWS CloudShell

- Docker hat begrenzten Speicherplatz in einer Umgebung. Wenn Sie über große Einzelimages oder zu viele bereits vorhandene Docker-Images verfügen, kann dies zu Problemen führen, die Sie möglicherweise daran hindern, zusätzliche Images abzurufen, zu erstellen oder auszuführen. Weitere Informationen zu Docker finden Sie im Docker-Dokumentationsleitfaden.
- Docker wird nur in bestimmten Regionen unterstützt. Informationen darüber, welche Regionen von Docker unterstützt werden, finden Sie unter Docker-Regionen.
- Wenn Sie bei der Verwendung von Docker mit auf Probleme stoßen AWS CloudShell, finden Sie im Abschnitt zur Fehlerbehebung dieses Handbuchs Informationen darüber, wie Sie diese Probleme möglicherweise beheben können.

Arbeiten mit Barrierefreiheitsfunktionen fürAWS CloudShell

In diesem Thema wird beschrieben, wie Sie Barrierefreiheitsfunktionen verwenden fürCloudShell. Sie können eine Tastatur verwenden, um durch die fokussierbaren Elemente auf der Seite zu navigieren. Sie können auch das Erscheinungsbild von anpassenCloudShell, einschließlich Schriftgrößen und Benutzeroberflächenthemen.

Tastaturnavigation inCloudShell

Um durch die fokussierbaren Elemente auf der Seite zu navigieren, drücken SieTab.

CloudShellFunktionen zur Barrierefreiheit im Terminal

Sie können die verwendenTabTaste in den folgenden Modi:

- Terminalmodus (Standard)— In diesem Modus erfasst das Terminal IhreTabSchlüsseleingabe. Wenn der Fokus auf dem Terminal liegt, drücken SieTabum nur auf die Funktionalität des Terminals zuzugreifen.
- Navigationsmodus— In diesem Modus erfasst das Terminal Ihre nichtTabSchlüsseleingabe. DrückenTabum durch die fokussierbaren Elemente auf der Seite zu navigieren.

Um zwischen dem Terminalmodus und dem Navigationsmodus zu wechseln, drücken SieCtrl+M. Nachdem du zurückgeschaltet hast,Reiter: Navigationerscheint in der Kopfzeile, und Sie können das verwendenTabTaste, um durch die Seite zu navigieren.

Um zum Terminalmodus zurückzukehren, drücken SieCtrl+M. Oder wähleXnebenRegisterkarte: Navigation.

> **Note**
>
> DerzeitCloudShellFunktionen zur Barrierefreiheit von Terminals sind auf Mobilgeräten nicht verfügbar.

Auswahl von Schriftgrößen und Benutzeroberflächenthemen inCloudShell

Sie können das Erscheinungsbild von anpassenCloudShellum Ihren visuellen Vorlieben gerecht zu werden.

- Schriftgröße— Wählen Sie ausAm kleinsten,Klein,Mittel,Groß, undGrößteSchriftgrößen im Terminal. Weitere Informationen zum Ändern der Schriftgröße finden Sie unterthe section called “Schriftgröße ändern”.
- Thema— Wählen Sie zwischenLeichtundDunkelThemen der Benutzeroberfläche. Weitere Informationen zum Ändern des Benutzeroberflächenthemas finden Sie unterthe section called “Das Design der Benutzeroberfläche ändern”.

Zusammenarbeit mitAWS Diensten inAWS CloudShell

Ein Hauptvorteil vonAWS CloudShell ist, dass Sie damit IhreAWS Dienste über die Befehlszeilenschnittstelle verwalten können. Das bedeutet, dass Sie keine Tools herunterladen und installieren oder Ihre Anmeldeinformationen lokal konfigurieren müssen. Beim Start wird eine Rechenumgebung erstelltAWS CloudShell, in der die folgendenAWS Befehlszeilentools bereits installiert sind:

- AWS CLI
- AWS Elastic Beanstalk CLI
- Amazon ECS-
- AWS SAM

Und da Sie sich bereits angemeldet habenAWS, müssen Sie Ihre Anmeldeinformationen nicht lokal konfigurieren, bevor Sie Dienste nutzen können. Die Anmeldeinformationen, mit denen Sie sich angemeldet haben,AWS Management Console werden weitergeleitetAWS CloudShell.

Wenn Sie dieAWS Standardregion ändern möchtenAWS CLI, für die verwendet wird, können Sie den Wert ändern, der der`AWS_REGION` Umgebungsvariablen zugewiesen wurde. (Weitere Informationen finden Sie unter Geben Sie Ihren Standard für AWS-Region an AWS CLI.)

Im Rest dieses Themas wird veranschaulicht, wie Sie beginnen könnenAWS CloudShell, mit ausgewähltenAWS Diensten über die Befehlszeile zu interagieren.

AWS CLIBefehlszeilenbeispiele für ausgewählteAWS Dienste

Die folgenden Beispiele stellen nur einige der zahlreichenAWS Dienste dar, mit denen Sie mithilfe von Befehlen arbeiten können, die abAWS CLI Version 2 verfügbar sind. Eine vollständige Liste finden Sie in der AWS CLI Command Reference.

- DynamoDB
- AWS Cloud9
- Amazon EC2
- S3-Gletscher

DynamoDB

DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der schnelle und vorhersehbare Leistung nahtlos skalierbar bereitstellt. Die Implementierung des NoSQL-Modus durch diesen Dienst unterstützt Schlüsselwert- und Dokumentendatenstrukturen.

Der folgende`create-table` Befehl erstellt eine Tabelle im NoSQL-Stil, die`MusicCollection` in IhremAWS Konto benannt ist.

```
aws dynamodb create-table \
    --table-name MusicCollection \
    --attribute-definitions AttributeName=Artist,AttributeType=S
 AttributeName=SongTitle,AttributeType=S \
    --key-schema AttributeName=Artist,KeyType=HASH
 AttributeName=SongTitle,KeyType=RANGE \
    --provisioned-throughput ReadCapacityUnits=5,WriteCapacityUnits=5 \
    --tags Key=Owner,Value=blueTeam
```

Weitere Informationen finden Sie unter Verwenden von DynamoDB mit demAWS CLI im AWS Command Line InterfaceBenutzerhandbuch.

AWS Cloud9

AWS Cloud9ist eine Cloud-basierte integrierte Entwicklungsumgebung (IDE), mit der Sie Ihren Code in einem Browserfenster schreiben, ausführen und debuggen können. Die Umgebung verfügt über einen Code-Editor, einen Debugger und ein Terminal.

Der folgende`create-environment-ec2` Befehl erstellt eineAWS Cloud9 EC2-Entwicklungsumgebung mit den angegebenen Einstellungen. Der Service startet eine Amazon-EC2-Instance und stellt eine Verbindung von der Instance mit der Umgebung her.

```
aws cloud9 create-environment-ec2 --name my-demo-env --description "My demonstration
 development environment." --instance-type t2.micro --subnet-id subnet-1fab8aEX --
automatic-stop-time-minutes 60 --owner-arn arn:aws:iam::123456789012:user/MyDemoUser
```

Weitere Informationen finden Sie in der AWS Cloud9-Befehlszeilenreferenz.

Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webservice, der sichere und anpassbare Rechenkapazität in der Cloud bereitstellt. Der Service ist darauf ausgelegt, Cloud Computing zu erleichtern und zu erleichtern.

Der folgende`run-instances` Befehl startet eine t2.micro-Instance im angegebenen Subnetz einer VPC:

```
aws ec2 run-instances --image-id ami-xxxxxxxx --count 1 --instance-type t2.micro --key-name MyKeyPair --security-group-ids sg-903004f8 --subnet-id subnet-6e7f829e
```

Weitere Informationen finden Sie unter Verwenden von Amazon EC2 mit demAWS CLI im AWS Command Line InterfaceBenutzerhandbuch.

S3 Glacier

S3 Glacier und S3 Glacier Deep Archive sind sichere, langlebige und extrem kostengünstige Amazon S3 S3-Cloud-Speicherklassen für Datenarchivierung und Langzeit-Backups.

Mit dem folgenden`create-vault` Befehl wird ein Tresor erstellt — ein Container zum Speichern von Archiven:

```
aws glacier create-vault --vault-name my-vault --account-id -
```

Weitere Informationen finden Sie unter Verwenden von Amazon S3 Glacier mit demAWS CLI im AWS Command Line InterfaceBenutzerhandbuch.

AWSElastic Beanstalk

DieAWS Elastic Beanstalk CLI bietet eine Befehlszeilenschnittstelle zum einfacheren Erstellen, Aktualisieren und Überwachen von Umgebungen von einem lokalen Repository aus. In diesem Zusammenhang bezeichnet eine Umgebung eine Sammlung vonAWS Ressourcen, die eine Anwendungsversion ausführen.

Der folgende`create` Befehl erstellt eine neue Umgebung in einer benutzerdefinierten Amazon Virtual Private Cloud (VPC).

```
$ eb create dev-vpc --vpc.id vpc-0ce8dd99 --vpc.elbsubnets subnet-
b356d7c6,subnet-02f74b0c --vpc.ec2subnets subnet-0bb7f0cd,subnet-3b6697c1 --
vpc.securitygroup sg-70cff265
```

Weitere Informationen finden Sie in der EB CLI-Befehlsreferenz im AWS Elastic BeanstalkDeveloper Guide.

Amazon ECS-CLI

Die Amazon Elastic Container Service (Amazon ECS) -Befehlszeilenschnittstelle (CLI) bietet mehrere allgemeine Befehle. Diese sind darauf ausgelegt, Prozesse zum Erstellen, Aktualisieren und Überwachen von Clustern und Aufgaben von einer lokalen Entwicklungsumgebung aus zu erleichtern. (Ein Amazon-ECS- Cluster ist eine logische Gruppierung von Aufgaben oder Services.)

Der folgende`configure` Befehl konfiguriert die Amazon ECS-CLI, um eine Cluster-Konfiguration mit dem Namen zu erstellen`ecs-cli-demo`. Diese Cluster-Konfiguration verwendet`FARGATE` als Standardstarttyp für den`ecs-cli-demo` Cluster in`us-east-1 region`.

```
ecs-cli configure --region us-east-1 --cluster ecs-cli-demo --default-launch-type
 FARGATE --config-name ecs-cli-demo
```

Weitere Informationen finden Sie unter Amazon ECS-Befehlszeilenreferenz im Amazon Elastic Container Service-Entwicklerhandbuch.

AWS SAM CLI

AWS SAMCLI ist ein Befehlszeilentool, das mit einer AWS Serverless Application Model Vorlage und einem Anwendungscode arbeitet. Sie können damit mehrere Aufgaben ausführen. Dazu gehören das lokale Aufrufen von Lambda-Funktionen, das Erstellen eines Bereitstellungspakets für Ihre serverlose Anwendung und die Bereitstellung Ihrer serverlosen Anwendung in der AWS Cloud.

Der folgende`init` Befehl initialisiert ein neues SAM-Projekt, wobei die erforderlichen Parameter als Parameter übergeben werden:

```
sam init --runtime python3.7 --dependency-manager pip --app-template hello-world --name
 sam-app
```

Weitere Informationen finden Sie in der AWS SAMCLI-Befehlsreferenz im AWS Serverless Application ModelDeveloper Guide.

Anpassen IhresAWS CloudShellErfahrung

Sie können die folgenden Aspekte Ihres anpassenAWS CloudShellErfahrung:

- Anordnung der Tabs: Teilen Sie die Befehlszeilenschnittstelle in mehrere Spalten und Zeilen auf.
- Schriftgröße: Passen Sie die Größe des Befehlszeilentextes an.
- Farbthema: Wechselt zwischen hellem und dunklem Design.
- Sicheres Einfügen: Schalten Sie eine Funktion ein oder aus, bei der Sie mehrzeiligen Text überprüfen müssen, bevor er eingefügt wird.
- Tmux zur Sitzungswiederherstellung: Die Verwendung von tmux stellt Ihre Sitzung wieder her, bis die Sitzung inaktiv wird.

Sie können Ihre Shell-Umgebung auch erweitern umInstallation Ihrer eigenen SoftwareundÄndern von Start-Shell-Skripten.

Aufteilen der Befehlszeilenanzeige in mehrere Tabs

Führen Sie mehrere Befehle aus, indem Sie Ihre Befehlszeilenschnittstelle in mehrere Bereiche aufteilen.

> **Note**
>
> Nachdem Sie mehrere Registerkarten geöffnet haben, können Sie eine auswählen, in der Sie arbeiten möchten, indem Sie auf eine beliebige Stelle im Bereich Ihrer Wahl klicken. Sie können eine Registerkarte schließen, indem SiexSymbol, das sich neben dem Namen der Region befindet.

- WählenAktionenund eine der folgenden Optionen vonLayout der Registerkarten:
  - Neuer Tab: Fügt einen neuen Tab hinzu, der sich neben dem aktuell aktiven befindet.
  - In Zeilen aufgeteilt: Fügt eine neue Registerkarte in einer Zeile hinzu, die sich unter der aktuell aktiven befindet.
  - In Spalten aufgeteilt: Fügt eine neue Registerkarte in einer Spalte hinzu, die sich neben der aktuell aktiven befindet.

Wenn nicht genug Platz vorhanden ist, um jede Registerkarte vollständig anzuzeigen, scrollen Sie, um die gesamte Registerkarte zu sehen. Sie können auch die Teilungsbalken auswählen, die die Bereiche voneinander trennen, und sie mithilfe des Mauszeigers ziehen, um die Fenstergröße zu vergrößern oder zu verkleinern.

Schriftgröße ändern

Erhöhen oder verkleinern Sie den Text, der in der Befehlszeilenschnittstelle angezeigt wird.

1. Um das zu ändernAWS CloudShellTerminaleinstellungen, gehen Sie zuEinstellungen,Präferenzen.
2. Wählen Sie eine Textgröße. Ihre Optionen sindAm kleinsten,Klein,Mittel,Groß, undGrößte.

Das Design der Benutzeroberfläche ändern

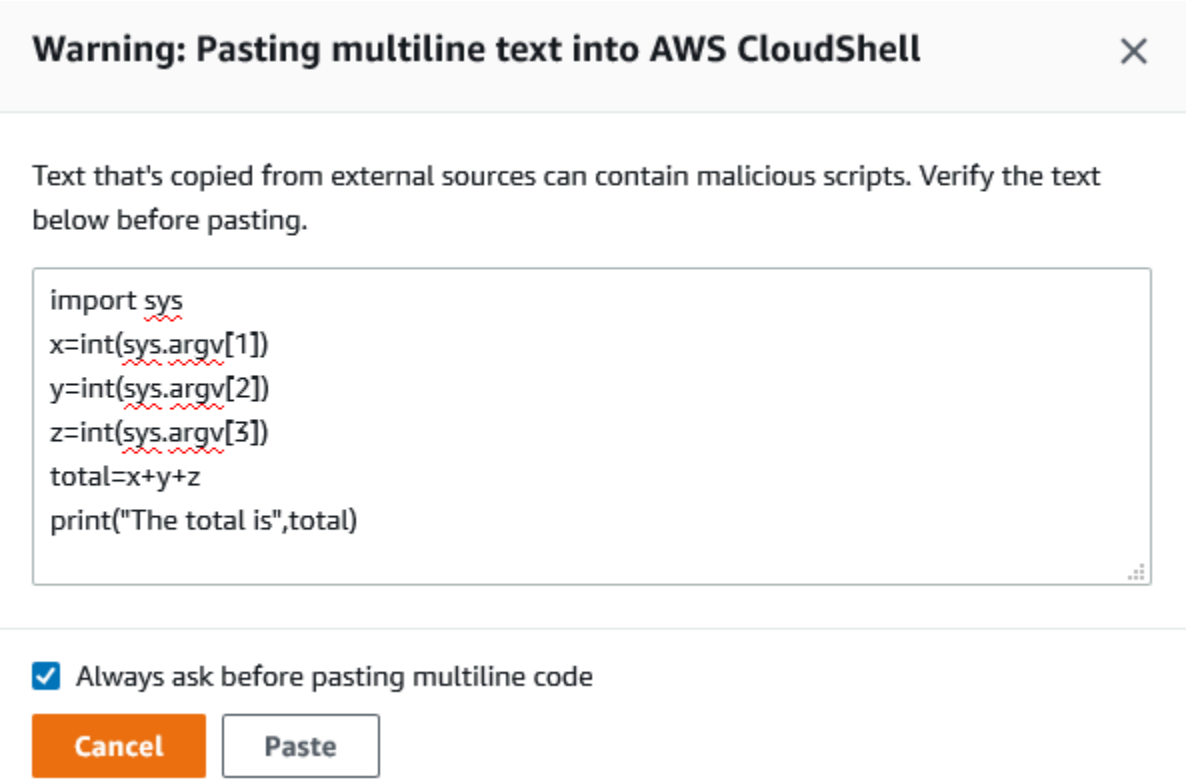
Wechseln Sie zwischen hellem und dunklem Design für die Befehlszeilenschnittstelle.

1. Um das zu ändernAWS CloudShellThema, gehe zuEinstellungen,Präferenzen.
2. WähleLichtoderDunkel.

Verwenden von Safe Paste für mehrzeiligen Text

Safe Paste ist eine Sicherheitsfunktion, mit der Sie überprüfen müssen, ob der mehrzeilige Text, den Sie in die Shell einfügen möchten, keine schädlichen Skripts enthält. Text, der von Websites Dritter kopiert wurde, kann versteckten Code enthalten, der unerwartete Verhaltensweisen in Ihrer Shell-Umgebung auslöst.

Im Dialogfeld „Sicheres Einfügen“ wird der vollständige Text angezeigt, den Sie in die Zwischenablage kopiert haben. Wenn Sie davon überzeugt sind, dass kein Sicherheitsrisiko besteht, wählen SieEinfügen.



Wir empfehlen, Safe Paste zu aktivieren, um potenzielle Sicherheitsrisiken in Skripts zu erkennen. Sie können diese Funktion ein- oder ausschalten, indem SieEinstellungen,Sicheres Einfügen aktivierenundDeaktivieren Sie Safe Paste.

Benutzentmuxzur Sitzungswiederherstellung

AWS CloudShellverwendet tmux, um die Sitzungen über einzelne oder mehrere Browser-Tabs hinweg wiederherzustellen. Wenn Sie die Browser-Tabs aktualisieren, wird Ihre Sitzung fortgesetzt, bis die Sitzung inaktiv wird. Weitere Informationen finden Sie unterWiederherstellung der Sitzung.

Verwendung AWS CloudShell in Amazon VPC

AWS CloudShell Mit einer Virtual Private Cloud (VPC) können Sie eine CloudShell Umgebung in Ihrer VPC erstellen. Für jede VPC-Umgebung können Sie eine VPC zuweisen, ein Subnetz hinzufügen und bis zu fünf Sicherheitsgruppen zuordnen. AWS CloudShell erbt die Netzwerkkonfiguration der VPC und ermöglicht es Ihnen, sie AWS CloudShell sicher innerhalb desselben Subnetzes wie andere Ressourcen in der VPC zu verwenden und eine Verbindung zu ihnen herzustellen.

Mit Amazon VPC können Sie AWS Ressourcen in einem logisch isolierten virtuellen Netzwerk starten, das Sie definiert haben. Dieses virtuelle Netzwerk entspricht weitgehend einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben, kann jedoch die Vorzüge der skalierbaren Infrastruktur von AWS nutzen. Weitere Informationen zu VPC finden Sie unter Amazon Virtual Private Cloud.

Betriebsbeschränkungen

AWS CloudShell VPC-Umgebungen haben die folgenden Einschränkungen:

- Sie können maximal zwei VPC-Umgebungen pro IAM-Prinzipal erstellen.
- Sie können einer VPC-Umgebung maximal fünf Sicherheitsgruppen zuweisen.
- Sie können die CloudShell Upload- und Download-Optionen im Aktionsmenü für VPC-Umgebungen nicht verwenden.

> **Note**
>
> Es ist möglich, Dateien aus VPC-Umgebungen hoch- oder herunterzuladen, die über andere CLI-Tools Zugriff auf den Ein- und Ausgang des Internets haben.

- VPC-Umgebungen unterstützen keinen persistenten Speicher. Speicher ist vergänglich. Daten und Home-Verzeichnis werden gelöscht, wenn eine aktive Umgebungssitzung endet.
- Ihre AWS CloudShell Umgebung kann nur dann eine Verbindung zum Internet herstellen, wenn sie sich in einem privaten VPC-Subnetz befindet.

> **Note**
>
> Öffentliche IP-Adressen werden CloudShell VPC-Umgebungen standardmäßig nicht zugewiesen. VPC-Umgebungen, die in öffentlichen Subnetzen mit Routingtabellen erstellt

wurden, die so konfiguriert sind, dass sie den gesamten Verkehr an Internet Gateway weiterleiten, haben keinen Zugriff auf das öffentliche Internet, aber private Subnetze, die mit Network Address Translation (NAT) konfiguriert sind, haben Zugriff auf das öffentliche Internet. VPC-Umgebungen, die in solchen privaten Subnetzen erstellt wurden, werden Zugang zum öffentlichen Internet haben.

- Um eine verwaltete CloudShell Umgebung für Ihr Konto bereitzustellen, AWS kann es Netzwerkzugriff auf die folgenden Dienste für den zugrunde liegenden Rechenhost bereitstellen:
  - Amazon S3
  - VPC-Endpunkte
    - com.amazonaws. <region>.ssm-Nachrichten
    - com.amazonaws. <region>.protokolle
    - com.amazonaws. <region>. km
    - com.amazonaws. <region>.execute-api
    - com.amazonaws. <region>.ecs-Telemetrie
    - com.amazonaws. <region>.ecs-Agent
    - com.amazonaws. <region>.ecs
    - com.amazonaws. <region>.ecr.dkr
    - com.amazonaws. <region>.ecr.api
    - com.amazonaws. <region>.codecatalyst.packages
    - com.amazonaws. <region>.codecatalyst.git
    - aws.api.global.codecatalyst

  Sie können den Zugriff auf diese Endpoints nicht einschränken, indem Sie Ihre VPC-Konfiguration ändern.

Eine CloudShell VPC-Umgebung erstellen

Voraussetzungen

Ihr Administrator muss Ihnen die erforderlichen IAM-Berechtigungen bereitstellen, damit Sie VPC-Umgebungen erstellen können. Weitere Informationen zum Aktivieren von Berechtigungen zum Erstellen von CloudShell VPC-Umgebungen finden Sie unterthe section called “Erforderliche IAM-Berechtigungen für die Erstellung und Verwendung von CloudShell VPC-Umgebungen”.

Um eine CloudShell VPC-Umgebung zu erstellen

1. Wählen Sie auf der CloudShell Konsolenseite das Pluszeichen und dann im Dropdownmenü die Option VPC-Umgebung erstellen aus.
2. Geben Sie auf der Seite VPC-Umgebung erstellen im Feld Name einen Namen für Ihre VPC-Umgebung ein.
3. Wählen Sie aus der Dropdownliste Virtual Private Cloud (VPC) eine VPC aus.
4. Wählen Sie aus der Dropdownliste Subnetz ein Subnetz aus.
5. Wählen Sie aus der Dropdownliste Sicherheitsgruppe eine oder mehrere Sicherheitsgruppen aus, die Sie Ihrer VPC-Umgebung zuweisen möchten.

   > **Note**
   >
   > Sie können maximal fünf Sicherheitsgruppen auswählen.

6. Wählen Sie Create, um Ihre VPC-Umgebung zu erstellen.
7. (Optional) Wählen Sie Aktionen und dann Details anzeigen aus, um die Details der neu erstellten VPC-Umgebung zu überprüfen. Die IP-Adresse Ihrer VPC-Umgebung wird in der Befehlszeile angezeigt.

Hinweise zur Verwendung von VPC-Umgebungen finden Sie unterErste Schritte.

Erforderliche IAM-Berechtigungen für die Erstellung und Verwendung von CloudShell VPC-Umgebungen

Um CloudShell VPC-Umgebungen zu erstellen und zu verwenden, muss der IAM-Administrator den Zugriff auf VPC-spezifische Amazon EC2 EC2-Berechtigungen aktivieren. In diesem Abschnitt sind die Amazon EC2 EC2-Berechtigungen aufgeführt, die zum Erstellen und Verwenden von VPC-Umgebungen erforderlich sind.

Um VPC-Umgebungen zu erstellen, muss die Ihrer Rolle zugewiesene IAM-Richtlinie die folgenden Amazon EC2 EC2-Berechtigungen enthalten:

- `ec2:DescribeVpcs`
- `ec2:DescribeSubnets`
- `ec2:DescribeSecurityGroups`

- `ec2:DescribeDhcpOptions`
- `ec2:DescribeNetworkInterfaces`

- `ec2:CreateTags`
- `ec2:CreateNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`

Wir empfehlen, auch Folgendes einzubeziehen:

- ec2:DeleteNetworkInterface

> **Note**
>
> Diese Berechtigung ist nicht verpflichtend, aber sie ist erforderlich, CloudShell um die von ihr erstellte ENI-Ressource zu bereinigen (ENIs, die für CloudShell VPC-Umgebungen erstellt wurden, sind mit einem ManagedByCloudShell Schlüssel gekennzeichnet). Wenn diese Berechtigung nicht aktiviert ist, müssen Sie die ENI-Ressource nach jeder Verwendung der CloudShell VPC-Umgebung manuell bereinigen.

IAM-Richtlinie gewährt vollen CloudShell Zugriff, einschließlich Zugriff auf VPC

Das folgende Beispiel zeigt, wie vollständige Berechtigungen, einschließlich Zugriff auf VPC, aktiviert werden können CloudShell für:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCloudShellOperations",
      "Effect": "Allow",
      "Action": [
        "cloudshell:*"
      ],
      "Resource": "*"
    },
```

```
    {
      "Sid": "AllowDescribeVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowCreateTagWithCloudShellKey",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        },
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": "ManagedByCloudShell"
        }
      }
    },
    {
      "Sid": "AllowCreateNetworkInterfaceWithSubnetsAndSG",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid": "AllowCreateNetworkInterfaceWithCloudShellTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface"
```

```
      ],
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": "ManagedByCloudShell"
        }
      }
    },
    {
      "Sid": "AllowCreateNetworkInterfacePermissionWithCloudShellTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/ManagedByCloudShell": ""
        }
      }
    },
    {
      "Sid": "AllowDeleteNetworkInterfaceWithCloudShellTag",
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/ManagedByCloudShell": ""
        }
      }
    }
  ]
}
```

Verwendung von IAM-Bedingungsschlüsseln für VPC-Umgebungen

Sie können CloudShell -spezifische Bedingungsschlüssel für VPC-Einstellungen verwenden, um zusätzliche Berechtigungskontrollen für Ihre VPC-Umgebungen bereitzustellen. Sie können auch die Subnetze und Sicherheitsgruppen angeben, die die VPC-Umgebung verwenden kann und welche nicht.

CloudShell unterstützt die folgenden Bedingungsschlüssel in IAM-Richtlinien:

- `CloudShell:VpcIds`— Erlaubt oder verweigert eine oder mehrere VPCs
- `CloudShell:SubnetIds`— Erlaube oder verbiete ein oder mehrere Subnetze
- `CloudShell:SecurityGroupIds`— Erlauben oder verweigern Sie eine oder mehrere Sicherheitsgruppen

> **Note**
>
> Wenn die Berechtigungen für Benutzer mit Zugriff auf öffentliche CloudShell Umgebungen geändert werden, um die `cloudshell:createEnvironment` Aktion einzuschränken, können sie weiterhin auf ihre bestehende öffentliche Umgebung zugreifen. Wenn Sie jedoch eine IAM-Richtlinie mit dieser Einschränkung ändern und ihren Zugriff auf die bestehende öffentliche Umgebung deaktivieren möchten, müssen Sie zuerst die IAM-Richtlinie mit der Einschränkung aktualisieren und dann sicherstellen, dass jeder CloudShell Benutzer in Ihrem Konto die bestehende öffentliche Umgebung manuell über die CloudShell Webbenutzeroberfläche löscht (Aktionen → Umgebung löschen CloudShell).

Beispielrichtlinien mit Bedingungsschlüsseln für VPC-Einstellungen

In den folgenden Beispielen wird gezeigt, wie Bedingungsschlüssel für VPC-Einstellungen verwendet werden. Nachdem Sie eine Richtlinienanweisung mit den gewünschten Einschränkungen erstellt haben, fügen Sie die Richtlinienanweisung für den -Zielbenutzer oder die Zielrolle an.

Stellen Sie sicher, dass Benutzer nur VPC-Umgebungen erstellen, und verweigern Sie die Erstellung öffentlicher Umgebungen

Um sicherzustellen, dass Benutzer nur VPC-Umgebungen erstellen können, verwenden Sie die Verweigerungsberechtigung, wie im folgenden Beispiel gezeigt:

```
{
  "Statement": [
    {
      "Sid": "DenyCloudShellNonVpcEnvironments",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
```

```
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "Null": {
          "cloudshell:VpcIds": "true"
        }
      }
    }
  ]
}
```

Benutzern den Zugriff auf bestimmte VPCs, Subnetze oder Sicherheitsgruppen verweigern

Um Benutzern den Zugriff auf bestimmte VPCs `StringEquals` zu verweigern, überprüfen Sie den Wert der `cloudshell:VpcIds`-Bedingung. Im folgenden Beispiel wird Benutzern der Zugriff auf und verweigert: `vpc-1` `vpc-2`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceOutOfVpc",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudshell:VpcIds": [
            "vpc-1",
            "vpc-2"
          ]
        }
      }
    }
  ]
}
```

Um Benutzern den Zugriff auf bestimmte VPCs `StringEquals` zu verweigern, überprüfen Sie den Wert der `cloudshell:SubnetIds`-Bedingung. Im folgenden Beispiel wird Benutzern der Zugriff auf und verweigert: `subnet-1` `subnet-2`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceOutOfVpc",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudshell:VpcIds": [
            "vpc-1",
            "vpc-2"
          ]
        }
      }
    }
  ]
}
```

Um Benutzern den Zugriff auf bestimmte VPCs `StringEquals` zu verweigern, überprüfen Sie den Wert der `cloudshell:SecurityGroupIds`-Bedingung. Im folgenden Beispiel wird Benutzern der Zugriff auf und verweigert: `sg-1` `sg-2`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceOutOfSecurityGroups",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
```

```
          "cloudshell:SecurityGroupIds": [
            "sg-1",
            "sg-2"
          ]
        }
      }
    }
  ]
}
```

Erlauben Sie Benutzern, Umgebungen mit bestimmten VPC-Konfigurationen zu erstellen

Um Benutzern Zugriff auf bestimmte VPCs zu gewähren, verwenden Sie, `StringEquals` um den Wert der `cloudshell:VpcIds` Bedingung zu überprüfen. Das folgende Beispiel ermöglicht Benutzern den Zugriff auf `vpc-1` und`vpc-2`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceStayInSpecificVpc",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudshell:VpcIds": [
            "vpc-1",
            "vpc-2"
          ]
        }
      }
    }
  ]
}
```

Um Benutzern Zugriff auf bestimmte VPCs zu gewähren, verwenden Sie, `StringEquals` um den Wert der `cloudshell:SubnetIds` Bedingung zu überprüfen. Das folgende Beispiel ermöglicht Benutzern den Zugriff auf `subnet-1` und`subnet-2`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceStayInSpecificSubnets",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "cloudshell:SubnetIds": [
            "subnet-1",
            "subnet-2"
          ]
        }
      }
    }
  ]
}
```

Um Benutzern Zugriff auf bestimmte VPCs zu gewähren, verwenden Sie, `StringEquals` um den Wert der `cloudshell:SecurityGroupIds` Bedingung zu überprüfen. Das folgende Beispiel ermöglicht Benutzern den Zugriff auf `sg-1` und`sg-2`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceStayInSpecificSecurityGroup",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "cloudshell:SecurityGroupIds": [
            "sg-1",
            "sg-2"
          ]
```

```
        }
      }
    }
  ]
}
```

Unterstützte Regionen für AWS CloudShell VPC

AWS CloudShell VPC-Umgebungen werden nur in den folgenden Regionen unterstützt:

- US East (Ohio)
- USA Ost (Nord-Virginia)
- USA West (Oregon)
- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Europe (Frankfurt)
- Europa (Irland)
- Europe (London)
- Europe (Paris)
- Südamerika (São Paulo)

Sicherheit für AWS CloudShell

Cloud-Sicherheit genießt bei Amazon Web Services (AWS) höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die auf die Anforderungen der sicherheitsempfindlichsten Unternehmen zugeschnitten sind. Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Im Modell der übergreifenden Verantwortlichkeit wird Folgendes mit „Sicherheit der Cloud“ bzw. „Sicherheit in der Cloud“ umschrieben:

Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der alle in der AWS Cloud angebotenen Dienste ausgeführt werden, und für die Bereitstellung von Diensten, die Sie sicher nutzen können. Unsere Sicherheitsverantwortung hat bei uns höchste Priorität AWS, und die Wirksamkeit unserer Sicherheit wird im Rahmen der AWS Compliance-Programme regelmäßig von externen Prüfern getestet und verifiziert.

Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem von Ihnen genutzten AWS Dienst und anderen Faktoren, wie der Sensibilität Ihrer Daten, den Anforderungen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften.

AWS CloudShell folgt dem Modell der gemeinsamen Verantwortung in Bezug auf die spezifischen AWS Dienste, die es unterstützt. Informationen zur AWS Servicesicherheit finden Sie auf der Dokumentationsseite zur AWS Servicesicherheit und zu den AWS Services, für die das Compliance-Programm gilt. AWS

In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AWS CloudShell , um Ihre Sicherheits- und Compliance-Ziele zu erreichen.

Themen

- AWS CloudShell Häufig gestellte Fragen zur Sicherheit

Datenschutz in AWS CloudShell

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS CloudShell. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der API AWS CloudShell oder den SDKs arbeiten oder diese anderweitig AWS-Services verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben,

die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung

Datenverschlüsselung bezieht sich auf den Schutz von Daten im Ruhezustand (während sie gespeichert sind AWS CloudShell) und bei der Übertragung (während der Übertragung zwischen AWS CloudShell und Service-Endpunkten).

Verschlüsselung im Ruhezustand mit AWS KMS

„Verschlüsselung im Ruhezustand“ bezieht sich auf den Schutz Ihrer Daten vor unbefugtem Zugriff durch deren Verschlüsselung während der Speicherung. Bei der Verwendung AWS CloudShell steht Ihnen kostenlos ein persistenter Speicher von 1 GB pro AWS Region zur Verfügung. Der persistente Speicher befindet sich in Ihrem Home-Verzeichnis (`$HOME`) und ist für Sie privat. Im Gegensatz zu kurzlebigen Umgebungsressourcen, die nach dem Ende jeder Shell-Sitzung wiederverwendet werden, bleiben Daten in Ihrem Basisverzeichnis erhalten.

Die Verschlüsselung der in gespeicherten Daten AWS CloudShell wird mithilfe von kryptografischen Schlüsseln implementiert, die von () bereitgestellt werden. AWS Key Management Service AWS KMS Dabei handelt es sich um einen verwalteten AWS Dienst zur Erstellung und Steuerung von Customer Master Keys (CMKs) — den Verschlüsselungsschlüsseln, die zur Verschlüsselung von Kundendaten verwendet werden, die in der Umgebung gespeichert sind. AWS CloudShell AWS CloudShell generiert und verwaltet kryptografische Schlüssel zur Verschlüsselung von Daten im Auftrag von Kunden.

Verschlüsselung während der Übertragung

Der Begriff „Verschlüsselung während der Übertragung“ bedeutet, dass Ihre Daten davor geschützt werden, abgefangen zu werden, während sie zwischen Kommunikationsendpunkten verschoben werden.

Standardmäßig wird die gesamte Datenkommunikation zwischen dem Webbrowser-Computer des Kunden und der Cloud-Umgebung verschlüsselt, indem alles über eine HTTPS/TLS-Verbindung gesendet AWS CloudShell wird.

Sie müssen nichts tun, um die Verwendung von HTTPS/TLS für die Kommunikation zu aktivieren.

Identity and Access Management für AWS CloudShell

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. CloudShell IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie tätig sind. CloudShell

Dienstbenutzer — Wenn Sie den CloudShell Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr CloudShell Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie in nicht auf eine Funktion zugreifen können CloudShell, finden Sie weitere Informationen unterFehlerbehebung bei CloudShell AWS-Identität und Zugriff.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für CloudShell Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf CloudShell. Es ist Ihre Aufgabe, zu bestimmen, auf welche CloudShell Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM

nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM nutzen kann CloudShell, finden Sie unterSo CloudShell arbeitet AWS mit IAM.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff darauf zu verwalten. CloudShell Beispiele für CloudShell identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS CloudShell

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges

Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.

- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige verwenden Funktionen in anderen. AWS-Services AWS-Services Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Auf Amazon EC2 ausgeführte Anwendungen — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie

ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern,

welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird,

ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So CloudShell arbeitet AWS mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf verwenden, sollten Sie sich darüber informieren CloudShell, mit welchen IAM-Funktionen Sie arbeiten können. CloudShell

IAM-Funktionen, die Sie mit AWS verwenden können CloudShell

IAM-Feature	CloudShell Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Nein
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Nein
Servicerollen	Nein
Serviceverknüpfte Rollen	Nein

Einen allgemeinen Überblick darüber, wie CloudShell und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für CloudShell

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für CloudShell

Beispiele für CloudShell identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS CloudShell

Ressourcenbasierte Richtlinien finden Sie in CloudShell

Unterstützt ressourcenbasierte Richtlinien	Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Politische Maßnahmen für CloudShell

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der CloudShell Aktionen finden Sie unter Von AWS definierte Aktionen CloudShell in der Service Authorization Reference. Einige Aktionen können mehr als eine API haben.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix CloudShell verwendet:

```
cloudshell
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "cloudshell:action1",
      "cloudshell:action2"
         ]
```

Beispiele für CloudShell identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS CloudShell

Politische Ressourcen für CloudShell

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der CloudShell Ressourcentypen und ihrer ARNs finden Sie unter Von AWS definierte Ressourcen CloudShell in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von AWS definierte Aktionen CloudShell.

Beispiele für CloudShell identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS CloudShell

Bedingungsschlüssel für Richtlinien für CloudShell

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der CloudShell Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS CloudShell in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS definierte Aktionen CloudShell.

Beispiele für CloudShell identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS CloudShell

ACLs in CloudShell

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit CloudShell

Unterstützt ABAC (Tags in Richtlinien)	Nein

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit CloudShell

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Wenn Sie die Rollen wechseln, verwenden Sie eine andere Umgebung. Sie können die Rollen innerhalb derselben AWS CloudShell Umgebung nicht wechseln.

Zugriffssitzungen weiterleiten für CloudShell

Unterstützt Forward Access Sessions (FAS)	Nein

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für CloudShell

Unterstützt Servicerollen	Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die CloudShell Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, CloudShell wenn Sie dazu eine Anleitung erhalten.

Dienstbezogene Rollen für CloudShell

Unterstützt serviceverknüpfte Rollen	Nein

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Beispiele für identitätsbasierte Richtlinien für AWS CloudShell

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Ressourcen zu erstellen oder zu ändern CloudShell. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden CloudShell, einschließlich des Formats der ARNs für jeden der Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS CloudShell in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der CloudShell-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand CloudShell Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und

Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der CloudShell-Konsole

Um auf die CloudShell AWS-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den CloudShell Ressourcen in Ihrem aufzulisten und einzusehen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die CloudShell Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die CloudShell `ConsoleAccess` oder die `ReadOnly` AWS verwaltete

Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI AWS OR-API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Fehlerbehebung bei CloudShell AWS-Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit CloudShell und IAM auftreten können.

Themen

Ich bin nicht berechtigt, eine Aktion durchzuführen in CloudShell

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `awes:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 awes:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `awes:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an CloudShell diese Person übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in auszuführen. CloudShell Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine CloudShell Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen CloudShell unterstützt werden, finden Sie unterSo CloudShell arbeitet AWS mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie im IAM-Benutzerhandbuch unter Kontenübergreifender Ressourcenzugriff in IAM.

AWS CloudShell Zugriff und Nutzung mit IAM-Richtlinien verwalten

Mit den Ressourcen für die Zugriffsverwaltung, die von AWS Identity and Access Management (IAM) bereitgestellt werden können, können Administratoren IAM-Benutzern Berechtigungen gewähren. Auf diese Weise können diese Benutzer auf die Funktionen der Umgebung zugreifen AWS CloudShell und diese nutzen. Administratoren können auch Richtlinien erstellen, die detailliert festlegen, welche Aktionen diese Benutzer in der Shell-Umgebung ausführen können.

Am schnellsten kann ein Administrator Benutzern Zugriff gewähren, indem er eine AWS verwaltete Richtlinie verwendet. Eine von AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. Die folgende AWS verwaltete Richtlinie für AWS CloudShell kann an IAM-Identitäten angehängt werden:

- AWS CloudShellFullAccess: Erteilt die Erlaubnis zur Nutzung AWS CloudShell mit vollem Zugriff auf alle Funktionen.

Die AWS CloudShellFullAccessRichtlinie verwendet das Platzhalterzeichen (*), um der IAM-Identität (Benutzer, Rolle oder Gruppe) vollen Zugriff auf Funktionen zu CloudShell gewähren. Weitere Informationen zu dieser Richtlinie finden Sie AWS CloudShellFullAccessim AWS Managed Policy User Guide.

> **Note**
>
> IAM-Identitäten mit den folgenden AWS verwalteten Richtlinien können ebenfalls gestartet werden. CloudShell Diese Richtlinien bieten jedoch umfangreiche Berechtigungen. Wir empfehlen daher, diese Richtlinien nur zu gewähren, wenn sie für die berufliche Rolle eines IAM-Benutzers unerlässlich sind.
>
> - Administrator: Bietet IAM-Benutzern vollen Zugriff und ermöglicht es ihnen, Berechtigungen für jeden Dienst und jede Ressource zu delegieren. AWS
> - Poweruser für Entwickler: Ermöglicht es IAM-Benutzern, Aufgaben zur Anwendungsentwicklung durchzuführen und Ressourcen und Dienste zu erstellen und zu konfigurieren, die die AWS bewusste Anwendungsentwicklung unterstützen.
>
> Weitere Informationen zum Anhängen verwalteter Richtlinien finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen (Konsole) im IAM-Benutzerhandbuch.

Verwaltung zulässiger Aktionen mithilfe benutzerdefinierter Richtlinien AWS CloudShell

Um die Aktionen zu verwalten, die ein IAM-Benutzer ausführen kann CloudShell, erstellen Sie eine benutzerdefinierte Richtlinie, die die CloudShellPolicy verwaltete Richtlinie als Vorlage verwendet. Sie können auch eine Inline-Richtlinie bearbeiten, die in die entsprechende IAM-Identität (Benutzer, Gruppe oder Rolle) eingebettet ist.

Sie können beispielsweise IAM-Benutzern Zugriff gewähren CloudShell, sie aber daran hindern, die Anmeldeinformationen für die CloudShell Umgebung weiterzuleiten, die für die Anmeldung verwendet werden. AWS Management Console

Important

Um AWS CloudShell von der aus zu starten AWS Management Console, benötigt ein IAM-Benutzer Berechtigungen für die folgenden Aktionen:

- `CreateEnvironment`
- `CreateSession`
- `GetEnvironmentStatus`
- `StartEnvironment`

Wenn eine dieser Aktionen durch eine angehängte Richtlinie nicht ausdrücklich zugelassen ist, wird beim Versuch, sie zu starten, ein IAM-Berechtigungsfehler zurückgegeben. CloudShell

AWS CloudShell Berechtigungen

Name	Beschreibung der gewährten Genehmigung	Zum Starten erforderlich CloudShell?
`cloudshell:CreateEnvironment`	Erstellt eine CloudShell Umgebung, ruft das Layout zu Beginn der	Ja

Name	Beschreibung der gewährten Genehmigung	Zum Starten erforderlich CloudShell?
	CloudShell Sitzung ab und speichert das aktuelle Layout aus der Webanwendung im Backend. Diese Berechtigung erwartet * nur den Wert für, `Resource` wie unter beschrieben. the section called “Beispiele für IAM-Richtlinien für CloudShell”	
`cloudshell:CreateSession`	Stellt eine Verbindung zu einer CloudShell Umgebung über den her AWS Management Console.	Ja
`cloudshell:GetEnvironmentStatus`	Lesen Sie den Status einer CloudShell Umgebung.	Ja
`cloudshell:DeleteEnvironment`	Löscht eine CloudShell Umgebung.	Nein
`cloudshell:GetFileDownloadUrls`	Generiert vorsignierte Amazon S3 S3-URLs, die zum Herunterladen von Dateien über CloudShell die CloudShell Weboberfläche verwendet werden. Dies ist für VPC-Umgebungen nicht verfügbar.	Nein

Name	Beschreibung der gewährten Genehmigung	Zum Starten erforderlich CloudShell?
`cloudshell:GetFileUploadUrls`	Generiert vorsignierte Amazon S3 S3-URLs, die zum Hochladen von Dateien über CloudShell die CloudShell Weboberfläche verwendet werden. Dies ist für VPC-Umgebungen nicht verfügbar.	Nein
`cloudshell:DescribeEnvironments`	Beschreibt die Umgebungen.	Nein
`cloudshell:PutCredentials`	Leitet die Anmeldeinformationen, die für die Anmeldung verwendet wurden, AWS Management Console an CloudShell weiter.	Nein
`cloudshell:StartEnvironment`	Startet eine CloudShell Umgebung, die gestoppt wurde.	Ja
`cloudshell:StopEnvironment`	Stoppt eine laufende CloudShell Umgebung.	Nein

Beispiele für IAM-Richtlinien für CloudShell

Die folgenden Beispiele zeigen, wie Richtlinien erstellt werden können, um einzuschränken, wer darauf zugreifen CloudShell kann. Die Beispiele zeigen auch die Aktionen, die in der Shell-Umgebung ausgeführt werden können.

Die folgende Richtlinie erzwingt eine vollständige Verweigerung des Zugriffs auf CloudShell und die zugehörigen Funktionen.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "DenyCloudShell",
        "Effect": "Deny",
        "Action": [
            "cloudshell:*"
        ],
        "Resource": "*"
    }]
}
```

Die folgende Richtlinie ermöglicht IAM-Benutzern den Zugriff, verhindert CloudShell jedoch, dass sie vorab signierte URLs für das Hoch- und Herunterladen von Dateien generieren. Benutzer können weiterhin Dateien in die und aus der Umgebung übertragen, indem sie `wget` beispielsweise Clients verwenden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Sid": "AllowUsingCloudshell",
        "Effect": "Allow",
        "Action": [
            "cloudshell:*"
        ],
        "Resource": "*"
    },
    {
        "Sid": "DenyUploadDownload",
        "Effect": "Deny",
        "Action": [
            "cloudshell:GetFileDownloadUrls",
            "cloudshell:GetFileUploadUrls"
        ],
        "Resource": "*"
    }]
}
```

Die folgende Richtlinie ermöglicht IAM-Benutzern den Zugriff CloudShell. Die Richtlinie verhindert jedoch, dass die Anmeldeinformationen, mit denen Sie sich angemeldet haben, AWS Management

Console an die CloudShell Umgebung weitergeleitet werden. IAM-Benutzer mit dieser Richtlinie müssen ihre Anmeldeinformationen darin CloudShell manuell konfigurieren.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Sid": "AllowUsingCloudshell",
        "Effect": "Allow",
        "Action": [
            "cloudshell:*"
        ],
        "Resource": "*"
    },
    {
        "Sid": "DenyCredentialForwarding",
        "Effect": "Deny",
        "Action": [
            "cloudshell:PutCredentials"
        ],
        "Resource": "*"
    }]
}
```

Die folgende Richtlinie ermöglicht es IAM-Benutzern, Umgebungen zu erstellen AWS CloudShell .

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "CloudShellUser",
        "Effect": "Allow",
        "Action": [
            "cloudshell:CreateEnvironment",
            "cloudshell:CreateSession",
            "cloudshell:GetEnvironmentStatus",
            "cloudshell:StartEnvironment"
        ],
        "Resource": "*"
     }]
}
```

Erforderliche IAM-Berechtigungen für die Erstellung und Verwendung von CloudShell VPC-Umgebungen

Um CloudShell VPC-Umgebungen zu erstellen und zu verwenden, muss der IAM-Administrator den Zugriff auf VPC-spezifische Amazon EC2 EC2-Berechtigungen aktivieren. In diesem Abschnitt sind die Amazon EC2 EC2-Berechtigungen aufgeführt, die zum Erstellen und Verwenden von VPC-Umgebungen erforderlich sind.

Um VPC-Umgebungen zu erstellen, muss die Ihrer Rolle zugewiesene IAM-Richtlinie die folgenden Amazon EC2 EC2-Berechtigungen enthalten:

- `ec2:DescribeVpcs`
- `ec2:DescribeSubnets`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeDhcpOptions`
- `ec2:DescribeNetworkInterfaces`

- `ec2:CreateTags`
- `ec2:CreateNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`

Wir empfehlen, auch Folgendes einzubeziehen:

- ec2:DeleteNetworkInterface

> **Note**
>
> Diese Berechtigung ist nicht verpflichtend, aber sie ist erforderlich, CloudShell um die von ihr erstellte ENI-Ressource zu bereinigen (ENIs, die für CloudShell VPC-Umgebungen erstellt wurden, sind mit einem ManagedByCloudShell Schlüssel gekennzeichnet). Wenn diese Berechtigung nicht aktiviert ist, müssen Sie die ENI-Ressource nach jeder Verwendung der CloudShell VPC-Umgebung manuell bereinigen.

IAM-Richtlinie gewährt vollen CloudShell Zugriff, einschließlich Zugriff auf VPC

Das folgende Beispiel zeigt, wie vollständige Berechtigungen, einschließlich Zugriff auf VPC, aktiviert werden können CloudShell für:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCloudShellOperations",
      "Effect": "Allow",
      "Action": [
        "cloudshell:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowDescribeVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowCreateTagWithCloudShellKey",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        },
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": "ManagedByCloudShell"
        }
      }
    },
```

```
    {
      "Sid": "AllowCreateNetworkInterfaceWithSubnetsAndSG",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid": "AllowCreateNetworkInterfaceWithCloudShellTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": "ManagedByCloudShell"
        }
      }
    },
    {
      "Sid": "AllowCreateNetworkInterfacePermissionWithCloudShellTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/ManagedByCloudShell": ""
        }
      }
    },
    {
      "Sid": "AllowDeleteNetworkInterfaceWithCloudShellTag",
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
```

```
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/ManagedByCloudShell": ""
        }
      }
    }
  ]
}
```

Verwendung von IAM-Bedingungsschlüsseln für VPC-Umgebungen

Sie können CloudShell -spezifische Bedingungsschlüssel für VPC-Einstellungen verwenden, um zusätzliche Berechtigungskontrollen für Ihre VPC-Umgebungen bereitzustellen. Sie können auch die Subnetze und Sicherheitsgruppen angeben, die die VPC-Umgebung verwenden kann und welche nicht.

CloudShell unterstützt die folgenden Bedingungsschlüssel in IAM-Richtlinien:

- `CloudShell:VpcIds`— Erlaubt oder verweigert eine oder mehrere VPCs
- `CloudShell:SubnetIds`— Erlaube oder verbiete ein oder mehrere Subnetze
- `CloudShell:SecurityGroupIds`— Erlauben oder verweigern Sie eine oder mehrere Sicherheitsgruppen

> **Note**
>
> Wenn die Berechtigungen für Benutzer mit Zugriff auf öffentliche CloudShell Umgebungen geändert werden, um die `cloudshell:createEnvironment` Aktion einzuschränken, können sie weiterhin auf ihre bestehende öffentliche Umgebung zugreifen. Wenn Sie jedoch eine IAM-Richtlinie mit dieser Einschränkung ändern und ihren Zugriff auf die bestehende öffentliche Umgebung deaktivieren möchten, müssen Sie zuerst die IAM-Richtlinie mit der Einschränkung aktualisieren und dann sicherstellen, dass jeder CloudShell Benutzer in Ihrem Konto die bestehende öffentliche Umgebung manuell über die CloudShell Webbenutzeroberfläche löscht (Aktionen → Umgebung löschen CloudShell).

Beispielrichtlinien mit Bedingungsschlüsseln für VPC-Einstellungen

In den folgenden Beispielen wird gezeigt, wie Bedingungsschlüssel für VPC-Einstellungen verwendet werden. Nachdem Sie eine Richtlinienanweisung mit den gewünschten Einschränkungen erstellt haben, fügen Sie die Richtlinienanweisung für den -Zielbenutzer oder die Zielrolle an.

Stellen Sie sicher, dass Benutzer nur VPC-Umgebungen erstellen, und verweigern Sie die Erstellung öffentlicher Umgebungen

Um sicherzustellen, dass Benutzer nur VPC-Umgebungen erstellen können, verwenden Sie die Verweigerungsberechtigung, wie im folgenden Beispiel gezeigt:

```
{
  "Statement": [
    {
      "Sid": "DenyCloudShellNonVpcEnvironments",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "Null": {
          "cloudshell:VpcIds": "true"
        }
      }
    }
  ]
}
```

Benutzern den Zugriff auf bestimmte VPCs, Subnetze oder Sicherheitsgruppen verweigern

Um Benutzern den Zugriff auf bestimmte VPCs `StringEquals` zu verweigern, überprüfen Sie den Wert der `cloudshell:VpcIds`-Bedingung. Im folgenden Beispiel wird Benutzern der Zugriff auf und verweigert: `vpc-1` `vpc-2`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceOutOfVpc",
```

```
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudshell:VpcIds": [
            "vpc-1",
            "vpc-2"
          ]
        }
      }
    }
  ]
}
```

Um Benutzern den Zugriff auf bestimmte VPCs `StringEquals` zu verweigern, überprüfen Sie den Wert der `cloudshell:SubnetIds`-Bedingung. Im folgenden Beispiel wird Benutzern der Zugriff auf und verweigert: `subnet-1` `subnet-2`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceOutOfVpc",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudshell:VpcIds": [
            "vpc-1",
            "vpc-2"
          ]
        }
      }
    }
  ]
}
```

Um Benutzern den Zugriff auf bestimmte VPCs `StringEquals` zu verweigern, überprüfen Sie den Wert der `cloudshell:SecurityGroupIds`-Bedingung. Im folgenden Beispiel wird Benutzern der Zugriff auf und verweigert: `sg-1` `sg-2`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceOutOfSecurityGroups",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "cloudshell:SecurityGroupIds": [
            "sg-1",
            "sg-2"
          ]
        }
      }
    }
  ]
}
```

Erlauben Sie Benutzern, Umgebungen mit bestimmten VPC-Konfigurationen zu erstellen

Um Benutzern Zugriff auf bestimmte VPCs zu gewähren, verwenden Sie, `StringEquals` um den Wert der `cloudshell:VpcIds` Bedingung zu überprüfen. Das folgende Beispiel ermöglicht Benutzern den Zugriff auf `vpc-1` und`vpc-2`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceStayInSpecificVpc",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Allow",
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "cloudshell:VpcIds": [
            "vpc-1",
            "vpc-2"
          ]
        }
      }
    }
  ]
}
```

Um Benutzern Zugriff auf bestimmte VPCs zu gewähren, verwenden Sie, `StringEquals` um den Wert der `cloudshell:SubnetIds` Bedingung zu überprüfen. Das folgende Beispiel ermöglicht Benutzern den Zugriff auf `subnet-1` und`subnet-2`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceStayInSpecificSubnets",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "cloudshell:SubnetIds": [
            "subnet-1",
            "subnet-2"
          ]
        }
      }
    }
  ]
}
```

Um Benutzern Zugriff auf bestimmte VPCs zu gewähren, verwenden Sie, `StringEquals` um den Wert der `cloudshell:SecurityGroupIds` Bedingung zu überprüfen. Das folgende Beispiel ermöglicht Benutzern den Zugriff auf `sg-1` und`sg-2`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceStayInSpecificSecurityGroup",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "cloudshell:SecurityGroupIds": [
            "sg-1",
            "sg-2"
          ]
        }
      }
    }
  ]
}
```

Berechtigungen für den Zugriff AWS-Services

CloudShell verwendet die IAM-Anmeldeinformationen, mit denen Sie sich bei der AWS Management Console angemeldet haben.

> **Note**
>
> Um die IAM-Anmeldeinformationen verwenden zu können, mit denen Sie sich bei der angemeldet haben AWS Management Console`cloudshell:PutCredentials`, benötigen Sie die entsprechende Berechtigung.

Diese Vorauthentifizierungsfunktion von CloudShell erleichtert die Verwendung. AWS CLI Ein IAM-Benutzer benötigt jedoch weiterhin explizite Berechtigungen für die AWS-Services , die über die Befehlszeile aufgerufen werden.

Nehmen wir zum Beispiel an, dass IAM-Benutzer Amazon S3 S3-Buckets erstellen und Dateien als Objekte in sie hochladen müssen. Sie können eine Richtlinie erstellen, die diese Aktionen ausdrücklich zulässt. Die IAM-Konsole bietet einen interaktiven visuellen Editor, der Sie durch den

Prozess der Erstellung eines Richtliniendokuments im JSON-Format führt. Nachdem die Richtlinie erstellt wurde, können Sie sie an die entsprechende IAM-Identität (Benutzer, Gruppe oder Rolle) anhängen.

Weitere Informationen zum Anhängen verwalteter Richtlinien finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen (Konsole) im IAM-Benutzerhandbuch.

Anmeldung und Überwachung AWS CloudShell

In diesem Thema wird beschrieben, wie Sie AWS CloudShell Aktivitäten und Leistung mit protokollieren und überwachen können CloudTrail.

Aktivität überwachen mit CloudTrail

AWS CloudShell ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder AWS-Service in ausgeführt wurden AWS CloudShell. CloudTrail erfasst alle API-Aufrufe AWS CloudShell als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS CloudShell Konsole und Code-Aufrufe an die AWS CloudShell API.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon Simple Storage Service (Amazon S3) -Bucket aktivieren. Dazu gehören Ereignisse für AWS CloudShell.

Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von CloudTrail gesammelten Informationen können Sie eine Vielzahl von Informationen zu einer Anfrage ermitteln. Sie können beispielsweise ermitteln, welche Anfrage an AWS gestellt wurde CloudShell, Sie können die IP-Adresse ermitteln, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat und wann sie gestellt wurde.

AWS CloudShell in CloudTrail

In der folgenden Tabelle sind die AWS CloudShell Ereignisse aufgeführt, die in der CloudTrail Protokolldatei gespeichert sind.

> **Note**
>
> AWS CloudShell Ereignis, das Folgendes beinhaltet:
>
> - *gibt an, dass es sich um einen API-Aufruf handelt, der nicht mutiert (schreibgeschützt).

- Das Wort `Environment` bezieht sich auf den Lebenszyklus der Rechenumgebung, in der das Shell-Erlebnis gehostet wird.
- Das Wort `Layout` stellt alle Browser-Tabs im CloudShell Terminal wieder her.

CloudShell Ereignisse in CloudTrail

Ereignisname	Beschreibung
`createEnvironment`	Tritt auf, wenn eine CloudShell Umgebung erstellt wird.
`createSession`	Tritt auf, wenn eine CloudShell Umgebung über den verbunden wird AWS Management Console.
`deleteEnvironment`	Tritt auf, wenn eine CloudShell Umgebung gelöscht wird.
`deleteSession`	Tritt auf, wenn die Sitzung auf der CloudShell Registerkarte, die auf der aktuellen Browserre gisterkarte ausgeführt wird, gelöscht wird.
`getEnvironmentStatus*`	Tritt auf, wenn der Status einer CloudShell Umgebung abgerufen wird.
`getFileDownloadUrls*`	Tritt auf, wenn vorsignierte Amazon S3 S3-URLs generiert werden, die zum Herunterladen von Dateien CloudShell über die CloudShell Weboberfläche verwendet werden.
`getFileUploadUrls*`	Tritt auf, wenn vorsignierte Amazon S3 S3-URLs generiert werden, die zum Hochladen von Dateien CloudShell über die CloudShell Weboberfläche verwendet werden.
`cloudshell:DescribeEnvironments`	Beschreibt die Umgebungen.

Ereignisname	Beschreibung
`getLayout*`	Tritt auf, wenn das CloudShell Layout zu Beginn der Sitzung abgerufen wird.
`putCredentials`	Tritt auf, wenn die Anmeldeinformationen, mit denen Sie sich bei AWS Management Console To angemeldet haben, weitergeleitet CloudShel l werden.
`redeemCode*`	Tritt auf, wenn der Workflow zum Abrufen des Aktualisierungstokens in der CloudShel l Umgebung beginnt. Sie können dieses Token später im `putCredentials` Befehl verwenden, um auf die CloudShell Umgebung zuzugreifen.
`sendHeartBeat`	Tritt auf, um zu bestätigen, dass die CloudShell Sitzung aktiv ist.
`startEnvironment`	Tritt auf, wenn eine CloudShell Umgebung gestartet wird.
`stopEnvironment`	Tritt auf, wenn eine laufende CloudShell Umgebung gestoppt wird.
`updateLayout`	Tritt auf, wenn das aktuelle Layout aus der Webanwendung im Backend gespeichert wird.

Ereignisse, die das Wort „Layout“ enthalten, stellen alle Browser-Tabs im CloudShell Terminal wieder her.

EventBridge Regeln für AWS CloudShell Aktionen

Mit EventBridge Regeln geben Sie eine Zielaktion an, die ausgeführt werden soll, wenn EventBridge ein Ereignis eintrifft, das der Regel entspricht. Sie können eine Regel definieren, die eine Zielaktion festlegt, die auf der Grundlage einer AWS CloudShell Aktion ausgeführt werden soll, die als Ereignis in einer CloudTrail Protokolldatei aufgezeichnet wurde.

Sie können beispielsweise EventBridge Regeln mit dem AWS CLI `put-rule` Befehl erstellen. Ein `put-rule` Aufruf muss mindestens ein EventPattern Oder enthalten ScheduleExpression. Regeln mit EventPatterns werden ausgelöst, wenn ein entsprechendes Ereignis beobachtet wird. Die EventPattern vier AWS CloudShell Ereignisse:

```
{ "source": [ "aws.cloudshell" ], "detail-type": [ "AWS API Call via CloudTrail" ],
 "detail": { "eventSource": [ "cloudshell.amazonaws.com" ] } }
```

Weitere Informationen finden Sie unter Ereignisse und Ereignismuster EventBridge im EventBridge Amazon-Benutzerhandbuch.

Überprüfung der Einhaltung der Vorschriften für AWS CloudShell

Externe Prüfer bewerten die Sicherheit und Konformität von AWS Services im Rahmen mehrerer AWS Compliance-Programme.

AWS CloudShell fällt in den Geltungsbereich der folgenden Compliance-Programme:

SOC

AWS Bei Berichten über System- und Organisationskontrollen (SOC) handelt es sich um unabhängige Prüfungsberichte von Drittanbietern, aus denen hervorgeht, wie wichtige Compliance-Kontrollen und -Ziele AWS erreicht werden.

Service	SDK	SOC 1,2,3
AWS CloudShell	CloudShell	✓

PCI

Der Payment Card Industry Data Security Standard (PCI DSS) ist ein firmeneigener Informationssicherheitsstandard, der vom PCI Security Standards Council verwaltet wird, der von American Express, Discover Financial Services, JCB International, MasterCard Worldwide und Visa Inc. gegründet wurde.

Service	SDK	PCI
AWS CloudShell	CloudShell	✓

ISO- und CSA STAR-Zertifizierungen und Dienstleistungen

AWS ist für die Einhaltung von ISO/IEC 27001:2013, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 9001:2015 und CSA STAR CCM v4.0 zertifiziert.

Service	SDK	ISO- und CSA STAR-Zertifizierungen und Dienstleistungen
AWS CloudShell	CloudShell	✓

FedRamp

Das Federal Risk and Authorization Management Program (FedRAMP) ist ein US-Bundesprogramm, das einen Standardansatz für die Sicherheitsprüfung, Autorisierung und die laufende Überwachung von Cloud-Produkten und -Services bereitstellt..

Service	SDK	FedRAMP Moderate (Osten/West)	FedRAMP Hoch () GovCloud
AWS CloudShell	CloudShell	✓	✓

DoD CC SRG

Der Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) bietet einen standardisierten Bewertungs- und Autorisierungsprozess für Cloud-Serviceanbieter (CSPs), um eine vorläufige DoD-Autorisierung zu erhalten, damit sie mit DoD-Kunden zusammenarbeiten können.

Services, die eine DoD-CC-SRG-Bewertung und -Autorisierung durchlaufen, haben den folgenden Status:

- Bewertung durch eine externe Bewertungsorganisation (3PAO): Dieser Service wird derzeit von unserem externen Prüfer bewertet.
- Überprüfung durch das Joint Authorization Board (JAB): Dieser Service wird derzeit einer JAB-Überprüfung unterzogen.

- Überprüfung durch die Defense Information Systems Agency (DISA): Dieser Dienst wird derzeit einer DISA-Überprüfung unterzogen.

Service	SDK	DoD CC SRG IL2 (Ost/West)	DoD CC SRG IL (2) GovCloud	DoD CC SRG IL (4) GovCloud	DoD CC SRG IL5 () GovCloud	DoD CC SRG IL6 (Geheime Region)AWS
AWS CloudShell	CloudShell	3PAO-Bewertung	N/A	–	–	–

HIPAA BAA

Der Health Insurance Portability and Accountability Act von 1996 (HIPAA) ist ein Bundesgesetz, das die Schaffung nationaler Standards zum Schutz vertraulicher Gesundheitsdaten von Patienten vor Offenlegung ohne deren Zustimmung oder Wissen vorschreibt.

AWS ermöglicht es betroffenen Unternehmen und ihren Geschäftspartnern, die HIPAA unterliegen, geschützte Gesundheitsinformationen (PHI) sicher zu verarbeiten, zu speichern und zu übertragen. Darüber hinaus AWS bietet das Unternehmen seit Juli 2013 ein standardisiertes Business Associate Addendum (BAA) für solche Kunden an.

Service	SDK	HIPAA BAA
AWS CloudShell	CloudShell	✓

IRAP

Mit dem Information Security Registered Assessors Program (IRAP) können australische Regierungskunden überprüfen, ob geeignete Kontrollmechanismen vorhanden sind, und das geeignete Verantwortungsmodell für die Erfüllung der Anforderungen des australischen Informationssicherheitshandbuchs (Information Security Manual, ISM), das vom Australian Cyber Security Centre (ACSC) ermitteln.

Service	Namespace*	IRAP geschützt
AWS CloudShell	N/A	✓

*Namespaces helfen Ihnen, Dienste in Ihrer Umgebung zu identifizieren. AWS Wenn Sie beispielsweise IAM-Richtlinien erstellen, mit Amazon Resource Names (ARNs) arbeiten und Protokolle lesen AWS CloudTrail .

MTCS

Multi-Tier Cloud Security (MTCS) ist ein operativer Sicherheitsmanagementstandard in Singapur (SPRING SS 584), der auf den ISO-Normen 27001/02 für das Informationssicherheitsmanagementsystem (ISMS) basiert.

Service	SDK	USA Ost (Ohio)	USA Ost (Nord-Virginia)	Vereinigte Staaten von Amerika West (Oregon)	USA West (Nordkalifornien)	Singapur	Seoul
AWS CloudShell	CloudShell	✓	✓	✓	N/A	–	N/A

C5

Der Cloud Computing Compliance Controls Catalog (C5) ist ein vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) eingeführtes Prüfschema, mit dem Organisationen im Rahmen der „Sicherheitsempfehlungen für Cloud-Anbieter“ der deutschen Bundesregierung die betriebliche Sicherheit im Hinblick auf gängige Cyber-Angriffe bei der Nutzung von Cloud-Services nachweisen können.

Service	SDK	C5
AWS CloudShell	CloudShell	✓

ENS High

Das Akkreditierungssystem ENS (Esquema Nacional de Seguridad) wurde vom Ministerium für Finanzen und öffentliche Verwaltung und dem CCN (National Cryptologic Centre) entwickelt. Es umfasst die Grundprinzipien und Mindestanforderungen, die für einen angemessenen Schutz von Informationen erforderlich sind.

Service	SDK	ENS Hoch
AWS CloudShell	CloudShell	✓

FINMA

Die Eidgenössische Finanzmarktaufsicht (FINMA) ist die unabhängige Finanzmarktregulierungsbehörde der Schweiz. AWS Die Anpassung an die Anforderungen der FINMA zeigt unser kontinuierliches Engagement, die gestiegenen Erwartungen der Schweizer Finanzaufsichtsbehörden und Kunden an Cloud-Dienstleister zu erfüllen.

Service	SDK	FINMA
AWS CloudShell	CloudShell	✓

PiTuKri

AWS Die Anpassung an die PiTuKri Anforderungen zeigt unser kontinuierliches Engagement, die gestiegenen Erwartungen der finnischen Transport- und Kommunikationsagentur Traficom an Cloud-Dienstleister zu erfüllen.

Service	SDK	PiTuKri
AWS CloudShell	CloudShell	✓

Eine Liste der AWS Services, die in den Geltungsbereich bestimmter Compliance-Programme fallen, finden Sie unter AWS-Services in Umfang nach Compliance-Programm . Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern herunterladen, indem Sie AWS Artifact. Weitere Informationen finden Sie unter Herunterladen von Berichten in AWS Artifact.

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS CloudShell hängt von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance Kurzanleitungen zu — In diesen Bereitstellungshandbüchern werden architektonische Überlegungen erörtert und Schritte für die Implementierung sicherheits- und Compliance-orientierter Basisumgebungen beschrieben. AWS
- Whitepaper „Architecting for HIPAA Security and Compliance“ — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-konforme Anwendungen entwickeln können. AWS
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- Bewertung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus, sodass Sie überprüfen können AWS , ob Sie die Sicherheitsstandards und Best Practices der Branche einhalten.

Widerstandsfähigkeit in AWS CloudShell

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

AWS CloudShell Unterstützt zusätzlich zur AWS globalen Infrastruktur spezielle Funktionen zur Unterstützung Ihrer Datenausfallsicherheit und Backup-Anforderungen.

- Übergeben Sie Dateien, die Sie erstellt und zu AWS CodeCommit denen Sie hinzugefügt haben. Dies ist ein von Amazon Web Services gehosteter Versionskontrolldienst, mit dem Sie Assets privat in der Cloud speichern und verwalten können. Diese Ressourcen können aus Dokumenten, Quellcode und Binärdateien bestehen. Weitere Informationen finden Sie unter Tutorial: Verwendung CodeCommit inAWS CloudShell.
- Verwenden Sie AWS CLI Aufrufe, um Dateien in Ihrem Home-Verzeichnis in Amazon S3-Buckets anzugeben AWS CloudShell und sie als Objekte in Amazon S3 S3-Buckets hinzuzufügen. Ein Beispiel finden Sie im Tutorial „Erste Schritte“.

Sicherheit der Infrastruktur in AWS CloudShell

Als verwalteter Dienst AWS CloudShell ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff AWS CloudShell über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

> **Note**
>
> Installieren Sie standardmäßig AWS CloudShell automatisch Sicherheitspatches für die Systempakete Ihrer Computerumgebungen.

Konfiguration und Schwachstellenanalyse in AWS CloudShell

Es liegt in der Verantwortung des AWS CloudShell Benutzers, sicherzustellen, dass jegliche Software, die er in der Computerumgebung installiert hat, gepatcht und auf dem neuesten Stand ist.

Bewährte Sicherheitsmethoden für AWS CloudShell

Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht geeignet oder nicht ausreichend sind, sollten Sie sie als nützliche Überlegungen und nicht als bindend betrachten.

Einige bewährte Sicherheitsmethoden für AWS CloudShell

- Verwenden Sie IAM-Berechtigungen und -Richtlinien, um den Zugriff zu kontrollieren AWS CloudShell und sicherzustellen, dass Benutzer nur die Aktionen ausführen können (z. B. Dateien herunterladen und hochladen), die für ihre Rolle erforderlich sind. Weitere Informationen finden Sie unter AWS CloudShell Zugriff und Nutzung mit IAM-Richtlinien verwalten.
- Nehmen Sie keine sensiblen Daten wie Benutzer, Rollen oder Sitzungsnamen in Ihre IAM-Entitäten auf.
- Lassen Sie die Funktion „Sicheres Einfügen“ catch, um potenzielle Sicherheitsrisiken in Text zu erkennen, den Sie aus externen Quellen kopiert haben. Safe Paste ist standardmäßig aktiviert. Weitere Informationen finden Sie unter Verwenden von Safe Paste für mehrzeiligen Text.
- Machen Sie sich mit dem Modell der gemeinsamen Sicherheitsverantwortung vertraut, wenn Sie Anwendungen von Drittanbietern in der Computerumgebung von installiert haben AWS CloudShell.
- Bereiten Sie Rollback-Mechanismen vor, bevor Sie Shell-Skripts bearbeiten, die sich auf die Shell-Erfahrung des Benutzers auswirken. Weitere Informationen finden Sie unter Ändern Sie Ihre Shell mit Skripten.
- Speichern Sie Ihren Code sicher in einem Versionskontrollsystem, z. B. AWS CodeCommit.

AWS CloudShell Häufig gestellte Fragen zur Sicherheit

Antworten auf häufig gestellte Fragen zur Sicherheit in diesem Bereich AWS-Service.

- Welche AWS Prozesse und Technologien werden verwendet, wenn Sie eine Shell-Sitzung starten CloudShell und starten?

Welche AWS Prozesse und Technologien werden verwendet, wenn Sie eine Shell-Sitzung starten CloudShell und starten?

Bei der Anmeldung geben Sie Ihre IAM-Benutzeranmeldedaten ein. AWS Management Console Und wenn Sie CloudShell von der Konsolenoberfläche aus starten, werden diese Anmeldeinformationen für CloudShell API-Aufrufe verwendet, die eine Rechenumgebung für den Dienst erstellen. Anschließend wird eine AWS Systems Manager Sitzung für die Rechenumgebung erstellt und Befehle CloudShell an diese Sitzung gesendet.

Zurück zur Liste der häufig gestellten Fragen zur Sicherheit

Ist es möglich, den Netzwerkzugriff auf zu beschränken CloudShell?

In öffentlichen Umgebungen ist es nicht möglich, den Netzwerkzugriff einzuschränken. Wenn Sie den Netzwerkzugriff einschränken möchten, müssen Sie die Erlaubnis aktivieren, nur VPC-Umgebungen zu erstellen und die Erstellung öffentlicher Umgebungen zu verweigern.

Weitere Informationen finden Sie unter Stellen Sie sicher, dass Benutzer nur VPC-Umgebungen erstellen, und verweigern Sie die Erstellung öffentlicher Umgebungen.

Für CloudShell VPC-Umgebungen werden Netzwerkeinstellungen von Ihrer VPC übernommen. Durch die Verwendung CloudShell in einer VPC können Sie den Netzwerkzugriff Ihrer CloudShell VPC-Umgebung steuern.

Zurück zur Liste der häufig gestellten Fragen zur Sicherheit

Kann ich meine CloudShell Umgebung anpassen?

Sie können Dienstprogramme und andere Software von Drittanbietern für Ihre CloudShell Umgebung herunterladen und installieren. Nur Software, die in Ihrem $HOME Verzeichnis installiert ist, wird zwischen den Sitzungen beibehalten.

Gemäß dem Modell der AWS gemeinsamen Verantwortung sind Sie für die erforderliche Konfiguration und Verwaltung der von Ihnen installierten Anwendungen verantwortlich.

Zurück zur Liste der häufig gestellten Fragen zur Sicherheit

Wo ist mein **$HOME** Verzeichnis eigentlich gespeichert AWS Cloud?

Für öffentliche Umgebungen wird die Infrastruktur zum Speichern von Daten in Ihrem von Amazon S3 $HOME bereitgestellt.

In VPC-Umgebungen wird Ihr $HOME Verzeichnis gelöscht, wenn Ihre VPC-Umgebung das Zeitlimit überschreitet (nach 20 bis 30 Minuten Inaktivität) oder wenn Sie Ihre Umgebung löschen oder neu starten.

Zurück zur Liste der häufig gestellten Fragen zur Sicherheit

Ist es möglich, mein **$HOME** Verzeichnis zu verschlüsseln?

Nein, es ist nicht möglich, Ihr $HOME Verzeichnis mit Ihrem eigenen Schlüssel zu verschlüsseln. CloudShell Verschlüsselt jedoch Ihren $HOME Verzeichnisinhalt beim Speichern in Amazon S3.

Zurück zur Liste der häufig gestellten Fragen zur Sicherheit

Kann ich in meinem **$HOME** Verzeichnis einen Virenscan durchführen?

Derzeit ist es nicht möglich, einen Virenscan Ihres $HOME Verzeichnisses durchzuführen. Die Support für diese Funktion wird derzeit überprüft.

Zurück zur Liste der häufig gestellten Fragen zur Sicherheit

Kann ich den Ein- oder Ausgang von Daten für mich einschränken? CloudShell

Um den Ein- oder Ausgang einzuschränken, empfehlen wir die Verwendung einer CloudShell VPC-Umgebung. Das $HOME Verzeichnis einer VPC-Umgebung wird gelöscht, wenn Ihre VPC-Umgebung das Zeitlimit überschreitet (nach 20 bis 30 Minuten Inaktivität) oder wenn Sie Ihre Umgebung löschen oder neu starten. Im Menü Aktionen sind die Upload- und Download-Optionen für VPC-Umgebungen nicht verfügbar.

Zurück zur Liste der häufig gestellten Fragen zur Sicherheit

AWS CloudShellRechenumgebung: Spezifikationen und Software

Beim Start wird eine Rechenumgebung erstelltAWS CloudShell, die auf Amazon Linux 2023 basiert, um das Shell-Erlebnis zu hosten. Die Umgebung ist mit Rechenressourcen (vCPU und Speicher) konfiguriert und bietet eine breite Palette vorinstallierter Software, auf die über die Befehlszeilenschnittstelle zugegriffen werden kann. Sie können Ihre Standardumgebung auch konfigurieren, indem Sie Software installieren und Shell-Skripts ändern.

Ressourcen der Umgebung berechnen

Jeder AWS CloudShell Rechenumgebung werden die folgenden CPU- und Speicherressourcen zugewiesen:

- 1 vCPU (virtuelle Zentraleinheit)
- 2 GiB RAM

Und die Umgebung wird mit der folgenden Speicherkonfiguration bereitgestellt:

- 1 GB persistenter Speicher (der Speicher bleibt auch nach Ende der Sitzung bestehen)

Weitere Informationen finden Sie unter Persistenter Speicher.

CloudShell Netzwerkanforderungen

WebSockets

CloudShell hängt vom WebSocket Protokoll ab, das eine bidirektionale interaktive Kommunikation zwischen dem Webbrowser des Benutzers und dem CloudShell Dienst in der AWS Cloud ermöglicht. Wenn Sie einen Browser in einem privaten Netzwerk verwenden, wird der sichere Zugriff auf das Internet wahrscheinlich durch Proxyserver und Firewalls erleichtert. WebSocket Die Kommunikation kann normalerweise problemlos über Proxyserver erfolgen. In einigen Fällen verhindern WebSockets Proxyserver jedoch, dass sie ordnungsgemäß funktionieren. Wenn dieses Problem auftritt, meldet Ihre CloudShell Schnittstelle den folgenden Fehler:`Failed to open sessions : Timed out while opening the session`.

Wenn dieser Fehler wiederholt auftritt, überprüfen Sie in der Dokumentation Ihres Proxyservers, ob er so konfiguriert ist, dass er dies zulässt WebSockets. Sie können sich auch an den Systemadministrator Ihres Netzwerks wenden.

> **Note**
>
> Wenn Sie detaillierte Berechtigungen definieren möchten, indem Sie bestimmte URLs zulassen, können Sie einen Teil der URL hinzufügen, die in der AWS Systems Manager Sitzung verwendet wird, um eine WebSocket Verbindung zum Senden von Eingaben und Empfangen von Ausgaben herzustellen. (Ihre AWS CloudShell Befehle werden an diese Systems Manager Manager-Sitzung gesendet.)
> Das von Systems Manager dafür StreamUrl verwendete Format ist`wss://ssmmessages.`**`region`**`.amazonaws.com/v1/data-channel/`**`session-id`**`?stream=(input|output)`.
> Die Region stellt die Regionskennung für eine AWS Region dar, die von unterstützt wirdAWS Systems Manager, z. B. `us-east-2` für die Region USA Ost (Ohio).
> Da die Sitzungs-ID nach dem erfolgreichen Start einer bestimmten Systems Manager Manager-Sitzung erstellt wird, können Sie sie nur angeben, `wss://ssmmessages.region.amazonaws.com` wenn Sie Ihre URL-Zulassungsliste aktualisieren.
> Weitere Informationen zu diesem StartSessionVorgang finden Sie in der AWS Systems Manager API-Referenz.

Vorinstallierte Software

> **Note**
>
> Da die AWS CloudShell Entwicklungsumgebung regelmäßig aktualisiert wird, um Zugriff auf die neueste Software zu bieten, geben wir in dieser Dokumentation keine spezifischen Versionsnummern an. Stattdessen beschreiben wir, wie Sie überprüfen können, welche Version installiert ist. Um die installierte Version zu überprüfen, geben Sie den Programmnamen gefolgt von der `--version` Option ein (z. B.`git --version`).

Muscheln

Vorinstallierte Schalen

Name	Beschreibung	Versionsinformationen
Bash	Die Bash-Shell ist die Standard-Shell-Anwendung für. AWS CloudShell	`bash --version`
PowerShell (pwsh)	Es bietet eine Befehlsze ilenschnittstelle und Unterstüt zung für Skriptsprachen und PowerShell baut auf Microsoft .NET Command Language Runtime auf. PowerShell verwendet einfache Befehle namens`cmdlets`, die .NET-Objekte akzeptieren und zurückgeben.	`pwsh --version`
Z-Shell (zsh)	Die Z Shell, auch bekannt als`zsh`, ist eine erweiterte Version der Bourne Shell, die erweiterte Anpassung sunterstützung für Themes und Plugins bietet.	`zsh --version`

AWSBefehlszeilenschnittstellen (CLI)

CLI

Name	Beschreibung	Versionsinformationen
AWS CDKToolkit CLI	Das AWS CDK Toolkit, der CLI-Befehl`cdk`, ist das primäre Tool, das mit Ihrer AWS CDK App interagiert. Es führt Ihre	`cdk --version`

Name	Beschreibung	Versionsinformationen
	App aus, fragt das von Ihnen definierte Anwendungsmodell ab und erstellt und stellt die von der generierten Vorlagen bereit. AWS CloudFormation AWS CDK Weitere Informationen finden Sie unter Toolkit. AWS CDK	
AWS CLI	Das AWS CLI ist eine Befehlszeilenschnittstelle, mit der Sie mehrere AWS Dienste von der Befehlsze ile aus verwalten und mithilfe von Skripten automatisieren können. Weitere Informationen finden Sie unter Zusammena rbeit mitAWS Diensten inAWS CloudShell. Informationen darüber, wie Sie sicherstellen können, dass Sie die aktuelle up-to-date AWS CLI Version 2 verwenden, finden Sie unterInstallation AWS CLI in Ihrem Home-Verz eichnis.	`aws --version`

Name	Beschreibung	Versionsinformationen
EB-CLI	Die AWS Elastic Beanstalk CLI bietet eine Befehlsze ilenschnittstelle, um das Erstellen, Aktualisieren und Überwachen von Umgebunge n von einem lokalen Repositor y aus zu vereinfachen. Weitere Informationen finden Sie unter Verwenden der Elastic Beanstalk Beanstalk-Befehlszeilenschnittstelle (EB CLI) im AWS Elastic Beanstalk Entwicklerhandbuch.	`eb --version`
Amazon ECS-CLI	Die Befehlszeilenschnittstelle (CLI) von Amazon Elastic Container Service (Amazon ECS) bietet Befehle auf hoher Ebene, um die Erstellung, Aktualisierung und Überwachu ng von Clustern und Aufgaben zu vereinfachen. Weitere Informationen finden Sie unter Using the Amazon ECS Command Line Interface im Amazon Elastic Container Service Developer Guide.	`ecs-cli --version`

Name	Beschreibung	Versionsinformationen
AWS SAM-CLI	AWS SAMCLI ist ein Befehlszeilentool, das mit einer AWS Serverless Application Model Vorlage und einem Anwendung scode arbeitet. Sie können mehrere Aufgaben ausführen . Dazu gehören das lokale Aufrufen von Lambda-Fu nktionen, das Erstellen eines Bereitstellungspakets für Ihre serverlose Anwendung und die Bereitstellung Ihrer serverlosen Anwendung in der Cloud. AWS Weitere Informationen finden Sie in der AWS SAMCLI-Befehlsreferenz im AWS Serverless Application ModelDeveloper Guide.	`sam --version`

Name	Beschreibung	Versionsinformationen
AWS Tools for PowerShell	Dies AWS Tools for PowerShell sind PowerShell Module, die auf der Funktionalität basieren, die von der bereitgestellt wirdAWS SDK for .NET. Mit AWS Tools for PowerShell können Sie über die PowerShell Befehlszeile Skripte für Operationen auf Ihren AWS Ressourcen erstellen. AWS CloudShellinstalliert die modularisierte Version (AWS.Tools) von vor. AWS Tools for PowerShell Weitere Informationen finden Sie PowerShell im AWS Tools for PowerShellBenutzerhandbuch unter Verwenden der AWS-Tools für.	`pwsh --Command ' Get-Module -ListAvailable -Name AWS.Tools.Common'`

Laufzeiten und AWS-SDKs: Node.js und Python 3

Laufzeiten und AWS-SDKs

Name	Beschreibung	Versionsinformationen
Node.js (mit npm)	Node.js ist eine JavaScript Runtime, die die Anwendung asynchroner Programmiertechniken erleichtern soll. Weitere Informationen finden Sie in der Dokumentation	• Node.js: `node --version` • npm: `npm --version`

Name	Beschreibung	Versionsinformationen
	auf der offiziellen Website Node.js. npm ist ein Paketmanager, der Zugriff auf eine Online-Registrierung von JavaScrip t Modulen bietet. Weitere Informationen finden Sie in der Dokumentation auf der offiziell en npm-Website.	
SDK für JavaScript in Node.js	Das Software Development Kit (SDK) trägt zur Vereinfachung der Codierung bei, indem es JavaScript Objekte für AWS-Services wie Amazon S3, Amazon EC2, DynamoDB und Amazon SWF bereitste llt. Weitere Informationen finden Sie im AWS SDK for JavaScript-Entwicklerhandbu ch.	`npm -g ls --depth 0 2>/dev/null | grep aws-sdk`

Name	Beschreibung	Versionsinformationen
Python	Python 3 ist bereit, in der Shell-Umgebung verwendet zu werden. Python 3 gilt jetzt als Standardversion der Programmiersprache (die Unterstützung für Python 2 endete im Januar 2020). Weitere Informationen finden Sie in der Dokumentation auf der offiziellen Python-Seite. Ebenfalls vorinstalliert ist pip, der Paket-Installer für Python. Sie können dieses Befehlszeilenprogramm verwenden, um Python-Pakete aus Online-Indizes wie dem Python Package Index zu installieren. Weitere Informationen finden Sie in der Dokumentation der Python Packaging Authority.	• Python 3: `python3 --version` • pip: `pip3 --version`

Name	Beschreibung	Versionsinformationen
SDK für Python (Boto3)	Boto ist das Software Development Kit (SDK), mit dem Python-Entwickler z. B. Amazon EC2 und Amazon S3 erstellenAWS-Services, konfigurieren und verwalten . Das SDK bietet eine easy-to-use objektorientierte API sowie einfachen Zugriff darauf. AWS-Services Weitere Informationen finden Sie in der Boto3-Dokumentation.	`pip3 list | grep boto3`

Entwicklungstools und Shell-Dienstprogramme

Entwicklungstools und Shell-Dienstprogramme

Name	Beschreibung	Versionsinformationen
bash-completion	Bash-Completion ist eine Sammlung von Shell-Funktionen, die die automatische Vervollständigung von teilweise eingegebenen Befehlen oder Argumenten durch Drücken der Tabulatortaste ermöglichen. Sie finden die Pakete, die Bash-Completion unterstützt, in. `/usr/share/bash-completion/completions`	`dnf info bash-completion`

Name	Beschreibung	Versionsinformationen
	Um die automatische Vervollst ändigung für die Befehle eines Pakets einzurichten, muss die Programmdatei als Quelle bereitgestellt werden. Um beispielsweise die automatis che Vervollständigung für Git-Befehle einzurichten, fügen Sie die folgende Zeile hinzu, `.bashrc` damit die Funktion bei jedem AWS CloudShell Sitzungsstart verfügbar ist: `source /usr/share/bash-completion/completions/git` Wenn Sie benutzerdefinierte Vervollständigungsskripten verwenden möchten, fügen Sie sie Ihrem persistenten Home-Verzeichnis (`$HOME`) hinzu und beziehen Sie sie direkt darin `.bashrc`. Weitere Informationen finden Sie auf der README-Seite des Projekts unter GitHub.	

Name	Beschreibung	Versionsinformationen
CodeCommit Hilfsprogramm für Git	git-remote-codecommit ist ein Hilfsprogramm, das durch die Erweiterung von Git eine einfache Methode zum Pushen und Abrufen von Code aus CodeCommit Repositorys bereitstellt. Dies ist die empfohlene Methode zur Unterstützung von Verbindungen, die mit Verbundzugriff, Identitätsanbietern und temporären Anmeldeinformationen hergestellt werden. Weitere Informationen finden Sie unter Einrichtungsschritte für HTTPS-Verbindungen AWS CodeCommit mit git-remote-codecommit im AWS CodeCommitBenutzerhandbuch.	`pip3 list | grep git-remote-codecommit`
Git	Git ist ein verteiltes Versionskontrollsystem, das moderne Softwareentwicklungspraktiken durch Branch-Workflows und Content Staging unterstützt. Weitere Informationen finden Sie auf der Dokumentationsseite auf der offiziellen Website von Git.	`git --version`

Name	Beschreibung	Versionsinformationen
iputils	Das iputils-Paket enthält Hilfsprogramme für Linux-Netzwerke. Weitere Informationen zu den bereitgestellten Hilfsprogrammen finden Sie im iputils-Repository unter. GitHub	Beispiele für ein iputils-Tool: `arping -V`
jq	Das jq-Hilfsprogramm analysiert Daten im JSON-Format, um eine Ausgabe zu erzeugen, die durch Befehlszeilenfilter modifiziert wird. Weitere Informationen finden Sie im jq-Handbuch unter. GitHub	`jq --version`
kubectl	kubectl ist ein Befehlszeilentool für die Kommunikation mit der Steuerungsebene eines Kubernetes-Clusters mithilfe der Kubernetes-API.	`kubectl --version`
make	Das Make-Utility dient `makefiles` zur Automatisierung von Aufgabensätzen und zur Organisation der Codekompilierung. Weitere Informationen finden Sie in der GNU Make-Dokumentation.	`make --version`

Name	Beschreibung	Versionsinformationen
man	Der Befehl man stellt Handbuchseiten für Befehlsze ilenprogramme und Tools zur Verfügung. `man ls` Gibt beispielsweise die Handbuchs eite für den `ls` Befehl zurück, die den Inhalt von Verzeichn issen auflistet. Weitere Informationen finden Sie im Wikipedia-Eintrag auf der Manpage.	`man --version`
nano	nano ist ein kleiner und benutzerfreundlicher Editor für textbasierte Benutzero berflächen. Weitere Informati onen finden Sie in der GNU Nano-Dokumentation.	`nano --version`
procps	procps ist ein Systemver waltungsprogramm, mit dem Sie aktuell laufende Prozesse überwachen und stoppen können. Weitere Informationen finden Sie in der README-Datei, in der Programme aufgeführt sind, die mit procps ausgeführt werden können.	`ps --version`

Name	Beschreibung	Versionsinformationen
SSH-Client	SSH-Clients verwenden das Secure Shell-Protokoll für die verschlüsselte Kommunikation mit einem Remotecomputer. OpenSSH ist der SSH-Clien t, der vorinstalliert ist. Weitere Informationen finden Sie auf der OpenSSH-Seite, die von OpenBSD verwaltet wird.	`ssh -V`
sudo	Mit dem Sudo-Hilfsprogramm können Benutzer ein Programm mit den Sicherhei tsberechtigungen eines anderen Benutzers ausführen , in der Regel des Superuser s. Sudo ist nützlich, wenn Sie als Systemadministrato r Anwendungen installieren müssen. Weitere Informati onen finden Sie im Sudo-Hand buch.	`sudo --version`
tar	tar ist ein Befehlszeilenprogr amm, mit dem Sie mehrere Dateien in einer einzigen Archivdatei (oft als Tarball bezeichnet) gruppieren können. Weitere Informationen finden Sie in der GNU-Tar-D okumentation.	`tar --version`

Name	Beschreibung	Versionsinformationen
tmux	tmux ist ein Terminal-Multiplexer, mit dem Sie verschiedene Programme gleichzeitig in mehreren Fenstern ausführen können. Weitere Informationen finden Sie in einem Blog, der eine kurze Einführung in tmux bietet.	`tmux -V`
unzip	Weitere Informationen finden Sie unter zip/unzip.	
vim	vim ist ein anpassbarer Editor, mit dem Sie über eine textbasierte Oberfläche interagieren können. Weitere Informationen finden Sie in den Dokumentationsressourcen auf vim.org.	`vim --version`
wget	wget ist ein Computerprogramm, das verwendet wird, um Inhalte von Webservern abzurufen, die durch Endpunkte in der Befehlszeile angegeben werden. Weitere Informationen finden Sie in der GNU Wget-Dokumentation.	`wget --version`

Name	Beschreibung	Versionsinformationen

komprimieren/entpacken	Die Hilfsprogramme zum Komprimieren und Entpacken verwenden ein Archivdat eiformat, das eine verlustfr eie Datenkomprimierung ohne Datenverlust ermöglicht. Rufen Sie den Befehl zip auf, um Dateien in einem einzigen Archiv zu gruppieren und zu komprimieren. Verwenden Sie unzip, um Dateien aus einem Archiv in ein bestimmte s Verzeichnis zu extrahieren.	`unzip --version`
		
		`zip --version`

Name	Beschreibung	Versionsinformationen
Docker	Docker ist eine offene Plattform für die Entwicklung, den Versand und den Betrieb von Anwendungen. Docker ermöglicht es Ihnen, Ihre Anwendungen von Ihrer Infrastruktur zu trennen, sodass Sie Software schnell bereitstellen können. Es ermöglicht Ihnen, Dockerfiles im Inneren zu erstellen und AWS CloudShell Docker-Assets mit CDK zu erstellen. Informationen darüber, welche Regionen von Docker unterstützt werden, finden Sie unter Docker-Regionen. Sie sollten sich bewusst sein, dass Docker nur über begrenzten Speicherplatz in der Umgebung verfügt. Wenn Sie große Einzelbilder oder zu viele bereits vorhandene Docker-Images haben, kann dies zu Problemen führen. Weitere Informationen zu Docker finden Sie im Docker-Dokumentationsleitfaden.	`docker --version`

Installation AWS CLI in Ihrem Home-Verzeichnis

Wie die restliche Software, die in Ihrer CloudShell Umgebung vorinstalliert ist, wird das AWS CLI Tool automatisch mit geplanten Upgrades und Sicherheitspatches aktualisiert. Wenn Sie sicherstellen

möchten, dass Sie über die meiste up-to-date Version von verfügenAWS CLI, können Sie das Tool manuell im Home-Verzeichnis der Shell installieren.

> **Important**
>
> Sie müssen Ihre Kopie von manuell AWS CLI im Home-Verzeichnis installieren, damit sie verfügbar ist, wenn Sie das nächste Mal eine CloudShell Sitzung starten. Diese Installation ist erforderlich, da Dateien, die zu Verzeichnissen außerhalb von hinzugefügt wurden, nach Abschluss einer Shell-Sitzung gelöscht `$HOME` werden. Außerdem wird diese Kopie von nach der AWS CLI Installation nicht automatisch aktualisiert. Mit anderen Worten, es liegt in Ihrer Verantwortung, Updates und Sicherheitspatches zu verwalten.
> Weitere Informationen zum Modell der AWS gemeinsamen Verantwortung finden Sie unterDatenschutz in AWS CloudShell.

So installieren Sie AWS CLI

1. Verwenden Sie in der CloudShell Befehlszeile den `curl` Befehl, um eine komprimierte Kopie der AWS CLI installierten Datei in die Shell zu übertragen:

   ```
   curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
   ```

2. Entpacken Sie den komprimierten Ordner:

   ```
   unzip awscliv2.zip
   ```

3. Um das Tool einem bestimmten Ordner hinzuzufügen, führen Sie das AWS CLI Installationsprogramm aus:

   ```
   sudo ./aws/install --install-dir /home/cloudshell-user/usr/local/aws-cli --bin-
   dir /home/cloudshell-user/usr/local/bin
   ```

   Wenn es erfolgreich installiert wurde, zeigt die Befehlszeile die folgende Meldung an:

   ```
   You can now run: /home/cloudshell-user/usr/local/bin/aws --version
   ```

4. Der Einfachheit halber empfehlen wir, dass Sie auch die `PATH` Umgebungsvariable aktualisieren, sodass Sie bei der Ausführung von `aws` Befehlen nicht den Pfad zu Ihrer Installation des Tools angeben müssen:

```
export PATH=/home/cloudshell-user/usr/local/bin:$PATH
```

> **Note**
>
> Wenn Sie diese Änderung rückgängig machen`PATH`, verwenden `aws` Befehle, die keinen angegebenen Pfad enthalten, standardmäßig die vorinstallierte Version AWS CLI von.

Software von Drittanbietern in Ihrer Shell-Umgebung installieren

> **Note**
>
> Wir empfehlen Ihnen, das Modell der gemeinsamen Sicherheitsverantwortung zu überprüfen, bevor Sie Drittanbieteranwendungen in AWS CloudShell der Computerumgebung installieren.

Standardmäßig verfügen alle AWS CloudShell Benutzer über Sudo-Berechtigungen. Daher können Sie den `sudo` Befehl verwenden, um Software zu installieren, die noch nicht in der Rechenumgebung der Shell verfügbar ist. Sie können ihn beispielsweise `sudo` zusammen mit dem DNF-Paketverwaltungsprogramm für die Installation verwenden`cowsay`, das ASCII-Grafikbilder einer Kuh mit der folgenden Meldung generiert:

```
sudo dnf install cowsay
```

Anschließend können Sie das neu installierte Programm starten, indem Sie Folgendes eingeben. `echo "Welcome to AWS CloudShell" | cowsay`

> **Important**
>
> Dienstprogramme zur Paketverwaltung wie dnf installieren Programme in Verzeichnissen (zum Beispiel)`/usr/bin`, die wiederverwendet werden, wenn Ihre Shell-Sitzung endet. Das bedeutet, dass zusätzliche Software pro Sitzung installiert und verwendet wird.

Ändern Sie Ihre Shell mit Skripten

Wenn Sie die Standard-Shell-Umgebung ändern möchten, können Sie ein Shell-Skript bearbeiten, das bei jedem Start der Shell-Umgebung ausgeführt wird. Das `.bashrc` Skript wird immer dann ausgeführt, wenn die Standard-Bash-Shell gestartet wird.

> **Warning**
>
> Wenn Sie Ihre `.bashrc` Datei falsch ändern, können Sie danach möglicherweise nicht mehr auf Ihre Shell-Umgebung zugreifen. Es empfiehlt sich, vor der Bearbeitung eine Kopie der Datei zu erstellen. Sie können das Risiko auch verringern, indem Sie bei der Bearbeitung `.bashrc` zwei Shells öffnen. Wenn Sie den Zugriff auf eine Shell verlieren, sind Sie immer noch in der anderen Shell angemeldet und können alle Änderungen rückgängig machen. Wenn Sie nach einer falschen Änderung `.bashrc` oder einer anderen Datei den Zugriff verlieren, können Sie AWS CloudShell zu den Standardeinstellungen zurückkehren, indem Sie Ihr Home-Verzeichnis löschen.

In diesem Verfahren ändern Sie das `.bashrc` Skript so, dass Ihre Shell-Umgebung automatisch zur Ausführung der Z-Shell wechselt.

1. Öffnen Sie das `.bashrc` mit einem Texteditor (z. B. Vim):

   ```
   vim .bashrc
   ```

2. Drücken Sie in der Editor-Oberfläche die Taste I, um mit der Bearbeitung zu beginnen, und fügen Sie dann Folgendes hinzu:

   ```
   zsh
   ```

3. Um die bearbeitete `.bashrc` Datei zu beenden und zu speichern, drücken Sie, Esc um in den Vim-Befehlsmodus zu wechseln, und geben Sie Folgendes ein:

   ```
   :wq
   ```

4. Verwenden Sie den `source` Befehl, um die Datei neu zu laden: `.bashrc`

   ```
   source .bashrc
   ```

Wenn die Befehlszeilenschnittstelle wieder verfügbar ist, hat sich das Eingabeaufforderungssymbol geändert und weist nun % darauf hin, dass Sie jetzt die Z-Shell verwenden.

AWS CloudShellMigration von Amazon Linux 2 zu Amazon Linux 2023

AWS CloudShell, das auf Amazon Linux 2 (AL2) basierte, wurde auf Amazon Linux 2023 (AL2023) migriert. Weitere Informationen zu AL2023 finden Sie unter Was ist Amazon Linux 2023 (AL2023) im Amazon Linux 2023-Benutzerhandbuch.

Mit AL2023 können Sie weiterhin mit allen von bereitgestellten Tools auf Ihre bestehende CloudShell Umgebung zugreifen. CloudShell Weitere Informationen zu verfügbaren Tools finden Sie unter Vorinstallierte Software.

AL2023 bietet mehrere Verbesserungen an Entwicklungstools, einschließlich neuerer Versionen von Paketen wie Node .js 18 und Python 3.9.

> **Note**
>
> In AL2023 ist Python 2 nicht mehr im Lieferumfang Ihrer CloudShell Umgebung enthalten.

Weitere Informationen zu den wichtigsten Unterschieden zwischen AL2 und AL2023 finden Sie unter Vergleich von Amazon Linux 2 und Amazon Linux 2023 im Amazon Linux 2023-Benutzerhandbuch.

Wenn Sie Fragen haben, wenden Sie sich an. AWS Support Sie können auch nach Antworten suchen und Fragen stellen in AWS re:Post. Wenn Sie teilnehmenAWS re:Post, müssen Sie sich möglicherweise anmeldenAWS.

AWS CloudShellHäufig gestellte Fragen zur Migration

Im Folgenden finden Sie Antworten auf einige häufig gestellte Fragen zur Migration von AL2 zu AL2023 mit. AWS CloudShell

- Wirkt sich diese Migration auf meine anderen AWS Ressourcen aus, z. B. auf AL2 Amazon EC2 EC2-Instances?

- Welche Pakete werden mit der Migration zu AL2023 geändert?
- Kann ich mich von der Migration abmelden?
- Kann ich ein Backup meiner AWS CloudShell Umgebung erstellen?

Wirkt sich diese Migration auf meine anderen AWS Ressourcen aus, z. B. auf AL2 Amazon EC2 EC2-Instances?

Außer Ihrer AWS CloudShell Umgebung ist kein anderer Dienst oder keine Ressource von dieser Migration betroffen. Dies schließt Ressourcen ein, die Sie möglicherweise von dort aus erstellt haben oder auf die Sie zugegriffen habenAWS CloudShell. Wenn Sie beispielsweise eine Amazon EC2 EC2-Instance erstellt haben, die auf AL2 läuft, wird diese nicht auf AL2023 migriert.

Welche Pakete wurden bei der Migration zu AL2023 geändert?

AWS CloudShellUmgebungen enthalten derzeit vorinstallierte Software. Eine vollständige Liste der vorinstallierten Software finden Sie unter Vorinstallierte Software. AWS CloudShellwird diese Pakete weiterhin ausliefern, mit Ausnahme von Python 2. Den vollständigen Unterschied zwischen den von AL2 und AL2023 bereitgestellten Paketen finden Sie unter Vergleich von AL2 und AL2023. Für Kunden mit spezifischen Paket- und Versionsanforderungen, die nach der Migration auf AL2023 nicht mehr erfüllt werden, empfehlen wir, sich an den AWS Support zu wenden, um eine Anfrage einzureichen.

Kann ich mich von der Migration abmelden

Die Antwort lautet NEIN. AWS CloudShellUmgebungen werden von verwaltetAWS, daher wurden alle Umgebungen auf AL2023 aktualisiert.

Kann ich ein Backup meiner AWS CloudShell Umgebung erstellen?

AWS CloudShellbehält das Home-Verzeichnis des Benutzers weiterhin bei. Weitere Informationen finden Sie unter Dienstkontingente und Einschränkungen für AWS CloudShell. Wenn Sie Dateien oder Konfigurationen in Ihrem Home-Ordner gespeichert haben und Sie dafür eine Sicherungskopie erstellen möchten, führen Sie Schritt 6: Erstellen einer Home-Verzeichnis-Backup aus.

Problembehebung AWS CloudShell

Bei der Verwendung AWS CloudShell können Probleme auftreten, z. B. wenn Sie wichtige Aufgaben über die Shell-Befehlszeilenschnittstelle starten CloudShell oder ausführen. In diesem Kapitel finden Sie Informationen zur Behebung einiger häufig auftretender Probleme.

Antworten auf eine Vielzahl von Fragen CloudShell zu finden Sie in den AWS CloudShell häufig gestellten Fragen. Sie können auch im AWS CloudShell Diskussionsforum nach Antworten suchen und Fragen stellen. Wenn Sie dieses Forum betreten, müssen Sie sich möglicherweise anmelden AWS. Sie können uns auch direkt kontaktieren.

Behebung von Fehlern

Wenn Sie auf einen der folgenden indizierten Fehler stoßen, können Sie die folgenden Lösungen verwenden, um diese Fehler zu beheben.

Themen

- Benutzer, die nur für VPC-Umgebungen CreateEnvironment berechtigt sind, haben auch Zugriff auf öffentliche AWS CloudShell Umgebungen

Die Umgebung konnte nicht gestartet werden. Um es erneut zu versuchen, aktualisieren Sie den Browser oder starten Sie ihn neu, indem Sie Aktionen, Neustart wählen AWS CloudShell

Problem: Wenn Sie versuchen, AWS CloudShell von der aus zu starten AWS Management Console, wird Ihnen der Zugriff verweigert, auch wenn Sie die Berechtigungen Ihres IAM-Administrators benötigen und Ihren Browser aktualisiert oder neu gestartet haben. CloudShell

Lösung: Wenden Sie sich an den AWS Support.

(zurück zum Seitenanfang)

Die Umgebung konnte nicht gestartet werden. Sie verfügen nicht über die erforderlichen Berechtigungen. Bitten Sie Ihren IAM-Administrator, Zugriff zu gewähren AWS CloudShell

Problem: Wenn Sie versuchen, AWS CloudShell von der aus zu starten AWS Management Console, wird Ihnen der Zugriff verweigert und Sie werden darüber informiert, dass Sie nicht über die erforderlichen Berechtigungen verfügen.

Ursache: Der IAM-Identität, die Sie für den Zugriff verwenden, AWS CloudShell fehlen die erforderlichen IAM-Berechtigungen.

Lösung: Bitten Sie Ihren IAM-Administrator, Ihnen die erforderlichen Berechtigungen zu erteilen. Dazu kann er entweder eine angehängte AWS verwaltete Richtlinie (AWSCloudShellFullAccess) oder eine eingebettete Inline-Richtlinie hinzufügen. Weitere Informationen finden Sie unter AWS CloudShell Zugriff und Nutzung mit IAM-Richtlinien verwalten.

(zurück zum Seitenanfang)

Zugriff auf die AWS CloudShell Befehlszeile nicht möglich

Problem: Nachdem Sie eine Datei geändert haben, die von der Rechenumgebung verwendet wird, können Sie nicht auf die Befehlszeile in zugreifen AWS CloudShell.

Lösung: Wenn Sie nach einer falschen Änderung `.bashrc` oder einer anderen Datei den Zugriff verlieren, können Sie AWS CloudShell zu den Standardeinstellungen zurückkehren, indem Sie Ihr Home-Verzeichnis löschen.

(zurück zum Seitenanfang)

Externe IP-Adressen konnten nicht gepingt werden

Problem: Wenn Sie einen Ping-Befehl von der Befehlszeile aus ausführen (z. B.`ping amazon.com`), erhalten Sie die folgende Meldung.

```
ping: socket: Operation not permitted
```

Ursache: Das Ping-Hilfsprogramm verwendet das Internet Control Message Protocol (ICMP), um Echoanforderungspakete an einen Zielhost zu senden. Es wartet auf die Antwort eines Echos vom Ziel. Da das ICMP-Protokoll in nicht aktiviert ist AWS CloudShell, funktioniert das Ping-Hilfsprogramm nicht in der Rechenumgebung der Shell.

Lösung: Da ICMP in nicht unterstützt wird, können Sie den folgenden Befehl ausführen AWS CloudShell, um Netcat zu installieren. Netcat ist ein Computernetzwerkprogramm zum Lesen und Schreiben von Netzwerkverbindungen mithilfe von TCP oder UDP.

```
sudo yum install nc
nc -zv www.amazon.com 443
```

(zurück zum Seitenanfang)

Bei der Vorbereitung Ihres Terminals sind einige Probleme aufgetreten

Problem: Wenn Sie versuchen, AWS CloudShell mit dem Microsoft Edge-Browser darauf zuzugreifen, können Sie keine Shell-Sitzung starten, und der Browser zeigt eine Fehlermeldung an.

Ursache: AWS CloudShell ist nicht mit früheren Versionen von Microsoft Edge kompatibel. Sie können AWS CloudShell mit den neuesten vier Hauptversionen der unterstützten Browser darauf zugreifen.

Lösung: Installieren Sie eine aktualisierte Version des Edge-Browsers von der Microsoft-Website.

(zurück zum Seitenanfang)

Die Pfeiltasten funktionieren nicht richtig in PowerShell

Problem: Im Normalbetrieb können Sie mit den Pfeiltasten in der Befehlszeilenschnittstelle navigieren und Ihren Befehlsverlauf vor- und zurückscannen. Wenn Sie jedoch in bestimmten Versionen von PowerShell on die Pfeiltasten drücken AWS CloudShell, werden Buchstaben möglicherweise falsch ausgegeben.

Ursache: Die Situation, dass Pfeiltasten Buchstaben falsch ausgeben, ist ein bekanntes Problem bei PowerShell 7.2.x-Versionen, die unter Linux ausgeführt werden.

Lösung: Um Escape-Sequenzen zu entfernen, die das Verhalten der Pfeiltasten verändern, bearbeiten Sie die PowerShell Profildatei und setzen Sie die `$PSStyle` Variable auf. `PlainText`

1. Geben Sie in der AWS CloudShell Befehlszeile den folgenden Befehl ein, um die Profildatei zu öffnen.

   ```
   vim ~/.config/powershell/Microsoft.PowerShell_profile.ps1
   ```

   > **Note**
   >
   > Wenn Sie bereits angemeldet sind PowerShell, können Sie die Profildatei auch mit dem folgenden Befehl im Editor öffnen.
   >
   > ```
   > vim $PROFILE
   > ```

2. Gehen Sie im Editor zum Ende des vorhandenen Texts der Datei, drücken Sie i, um in den Einfügemodus zu wechseln, und fügen Sie dann die folgende Anweisung hinzu.

   ```
   $PSStyle.OutputRendering = 'PlainText'
   ```

3. Nachdem Sie die Bearbeitung vorgenommen haben, drücken Sie, Esc um in den Befehlsmodus zu wechseln. Geben Sie anschließend den folgenden Befehl ein, um die Datei zu speichern und den Editor zu beenden.

   ```
   :wq
   ```

> **Note**
>
> Ihre Änderungen werden wirksam, wenn Sie das nächste Mal beginnen PowerShell.

(zurück zum Seitenanfang)

Nicht unterstützte Web Sockets führen dazu, dass Sitzungen nicht gestartet CloudShell werden können

Problem: Beim AWS CloudShell Startversuch erhalten Sie wiederholt die folgende Meldung:`Failed to open sessions : Timed out while opening the session`.

Ursache: CloudShell hängt vom WebSocket Protokoll ab, das eine wechselseitige interaktive Kommunikation zwischen Ihrem Webbrowser und AWS CloudShell ermöglicht. Wenn Sie einen Browser in einem privaten Netzwerk verwenden, wird der sichere Zugriff auf das Internet wahrscheinlich durch Proxyserver und Firewalls erleichtert. WebSocket Die Kommunikation kann normalerweise problemlos über Proxyserver erfolgen. In einigen Fällen verhindern WebSockets Proxyserver jedoch, dass sie ordnungsgemäß funktionieren. Wenn dieses Problem auftritt, CloudShell kann keine Shell-Sitzung gestartet werden, und der Verbindungsversuch läuft irgendwann ab.

Lösung: Ein Verbindungstimeout kann durch ein anderes als nicht WebSockets unterstütztes Problem verursacht werden. Wenn dies der Fall ist, aktualisieren Sie zunächst das Browserfenster, in dem sich die CloudShell Befehlszeilenschnittstelle befindet.

Wenn Sie nach der Aktualisierung immer noch Timeout-Fehler erhalten, lesen Sie in der Dokumentation Ihres Proxyservers nach. Stellen Sie außerdem sicher, dass Ihr Proxyserver so konfiguriert ist, dass er Web Sockets zulässt. Wenden Sie sich alternativ an den Systemadministrator Ihres Netzwerks.

> **Note**
>
> Angenommen, Sie möchten detaillierte Berechtigungen definieren, indem Sie bestimmte URLs auf eine Zulassungsliste setzen. Sie können einen Teil der URL hinzufügen, über die die AWS Systems Manager Sitzung eine WebSocket Verbindung zum Senden von Eingaben und Empfangen von Ausgaben herstellt. Ihre AWS CloudShell Befehle werden an diese Systems Manager Manager-Sitzung gesendet.

Das Format dafür StreamUrl , das von Systems Manager verwendet wird, ist `wss://ssmmessages.region.amazonaws.com/v1/data-channel/session-id?stream=(input|output)`.
Die Region stellt die Regionskennung für eine dar AWS-Region , die von unterstützt wird AWS Systems Manager. Dies `us-east-2` ist beispielsweise die Regionskennung für die Region USA Ost (Ohio).
Da die Sitzungs-ID erstellt wird, nachdem eine bestimmte Systems Manager Manager-Sitzung erfolgreich gestartet wurde, können Sie sie nur angeben, `wss://ssmmessages.region.amazonaws.com` wenn Sie Ihre URL-Zulassungsliste aktualisieren.
Weitere Informationen zu diesem StartSessionVorgang finden Sie in der AWS Systems Manager API-Referenz.

(zurück zum Seitenanfang)

Das **`AWSPowerShell.NetCore`** Modul konnte nicht importiert werden

Problem: Wenn Sie das importieren AWSPowerShell. NetCoreIm Modul PowerShell von `Import-Module -Name AWSPowerShell.NetCore` erhalten Sie die folgende Fehlermeldung:

Import-Module: Das angegebene Modul '. AWSPowerShell NetCore'wurde nicht geladen, da in keinem Modulverzeichnis eine gültige Moduldatei gefunden wurde.

Ursache: Das `AWSPowerShell.NetCore` Modul wurde durch die dienstspezifischen AWS.Tools-Module in ersetzt. AWS CloudShell

Lösung: Alle expliziten Importanweisungen sind möglicherweise nicht mehr erforderlich oder müssen in das zugehörige .Tools-Modul für jeden Dienst AWS geändert werden.

Example

Example

- In den meisten Fällen benötigen Sie keine explizite Importanweisung, solange keine.NET-Typen verwendet werden. Im Folgenden finden Sie Beispiele für Import-Anweisungen.
  - `Get-S3Bucket`
  - `(Get-EC2Instance).Instances`

- Wenn .Net-Typen verwendet werden, importieren Sie das Service-Level-Modul (`AWS.Tools.<Service>`). Es folgt ein Beispiel für die Syntax.

```
Import-Module -Name AWS.Tools.EC2
$InstanceTag = [Amazon.EC2.Model.Tag]::new("Environment","Dev")
```

```
Import-Module -Name AWS.Tools.S3
$LifecycleRule = [Amazon.S3.Model.LifecycleRule]::new()
```

Weitere Informationen finden Sie in der Ankündigung von Version 4 für. AWS Tools for PowerShell

(zurück zum Seitenanfang)

Docker läuft nicht bei der Verwendung AWS CloudShell

Problem: Docker läuft bei der Verwendung nicht richtig. AWS CloudShell Sie erhalten die folgende Fehlermeldung:`docker: Cannot connect to the Docker daemon at unix:///var/run/docker.sock. Is the docker daemon running?`.

Lösung: Versuchen Sie, Ihre Umgebung neu zu starten. Diese Fehlermeldung kann auftreten, wenn Sie Docker AWS CloudShell in einer Region ausführen, die Docker nicht unterstützt. Stellen Sie sicher, dass Sie Docker in einer unterstützten Region ausführen. Informationen darüber, in welchen Regionen die Verwendung von Docker-Containern unterstützt wird AWS CloudShell, finden Sie unter Docker-Regionen.

Docker hat keinen Speicherplatz mehr

Problem: Sie erhalten die folgende Fehlermeldung:`ERROR: failed to solve: failed to register layer: write [...]: no space left on device`.

Ursache: Das Dockerfile überschreitet den verfügbaren Speicherplatz in. AWS CloudShell Dies kann durch große Einzelbilder oder durch zu viele bereits vorhandene Docker-Images verursacht werden.

Lösung: Führen Sie `df -h` den Befehl aus, um die Festplattennutzung zu ermitteln. Führen Sie den Befehl aus`sudo du -sh /folder/folder1`, um die Größe bestimmter Ordner zu ermitteln, die Ihrer Meinung nach groß sein könnten, und erwägen Sie, andere Dateien zu löschen, um Speicherplatz freizugeben. Eine Option wäre, in Betracht zu ziehen, ungenutzte Docker-Images durch Ausführen `docker rmi` zu entfernen. Sie sollten sich bewusst sein, dass Docker nur über

begrenzten Speicherplatz in der Umgebung verfügt. Weitere Informationen zu Docker finden Sie im Docker-Dokumentationsleitfaden.

`docker push`hat eine Zeitüberschreitung und versucht es immer wieder

Problem: Bei der Ausführung kommt `docker push` es zu einem Timeout und es wird weiterhin erfolglos wiederholt.

Ursache: Dies kann auf fehlende Berechtigungen, das Verschieben in das falsche Repository oder auf eine fehlende Authentifizierung zurückzuführen sein.

Lösung: Um dieses Problem zu lösen, stellen Sie sicher, dass Sie zum richtigen Repository pushen. Führen Sie `docker login` die Datei aus, um sich ordnungsgemäß zu authentifizieren. Stellen Sie sicher, dass Sie über alle erforderlichen Berechtigungen für das Pushen in ein Amazon ECR-Repository verfügen.

Von meiner VPC-Umgebung aus kann nicht auf Ressourcen innerhalb der AWS CloudShell VPC zugegriffen werden

Problem: Während ich meine VPC-Umgebung verwende, kann ich nicht auf Ressourcen innerhalb der AWS CloudShell VPC zugreifen.

Ursache: Ihre AWS CloudShell VPC-Umgebung erbt die Netzwerkeinstellungen Ihrer VPC.

Lösung: Um dieses Problem zu beheben, stellen Sie sicher, dass Ihre VPC korrekt für den Zugriff auf Ihre Ressourcen eingerichtet ist. Weitere Informationen finden Sie in der VPC-Dokumentation Connect Sie Ihre VPC mit anderen Netzwerken und in der Network Access Analyzer-Dokumentation Network Access Analyzer. Sie finden die IPv4-Adresse, die die AWS CloudShell VPC-Umgebung verwendet, indem Sie den Befehl in Ihrer `ip -a` Umgebung in der Befehlszeile oder auf der VPC-Konsolenseite ausführen.

Die von AWS CloudShell für meine VPC-Umgebung verwendete ENI wurde nicht bereinigt

Problem: Die ENI, die von AWS CloudShell für meine VPC-Umgebung verwendet wurde, konnte nicht bereinigt werden.

Ursache: Die `ec2:DeleteNetworkInterface` Berechtigung ist für Ihre Rolle nicht aktiviert.

Lösung: Um dieses Problem zu beheben, stellen Sie sicher, dass die `ec2:DeleteNetworkInterface` Berechtigung für Ihre Rolle aktiviert ist, wie im folgenden Beispielskript gezeigt:

```
{
  "Effect": "Allow",
  "Action": [
    "ec2:DeleteNetworkInterface"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/ManagedByCloudShell": ""
    }
  },
  "Resource": "arn:aws:ec2:*:*:network-interface/*"
}
```

Benutzer, die nur für VPC-Umgebungen **`CreateEnvironment`** berechtigt sind, haben auch Zugriff auf öffentliche AWS CloudShell Umgebungen

Problem: Benutzer, die nur `CreateEnvironment` auf VPC-Umgebungen beschränkt sind, können auch auf öffentliche AWS CloudShell Umgebungen zugreifen.

Ursache: Wenn Sie die `CreateEnvironment` Berechtigungen nur für die Erstellung von VPC-Umgebungen einschränken und bereits eine öffentliche Umgebung erstellt haben, behalten Sie Ihren Zugriff auf die vorhandene öffentliche CloudShell Umgebung, bis diese Umgebung über die Webbenutzeroberfläche gelöscht wird. Wenn Sie diese jedoch noch nie CloudShell zuvor verwendet haben, haben Sie keinen Zugriff auf öffentliche Umgebungen.

Lösung: Um den Zugriff auf öffentliche AWS CloudShell Umgebungen einzuschränken, muss der IAM-Administrator zuerst die IAM-Richtlinie mit der Einschränkung aktualisieren. Anschließend muss der Benutzer die vorhandene öffentliche Umgebung manuell über die AWS CloudShell Webbenutzeroberfläche löschen. (Aktionen → CloudShell Umgebung löschen).

Unterstützte Browser für AWS CloudShell

In der folgenden Tabelle sind die für AWS CloudShell unterstützten Browser aufgeführt.

Webbrowser-Unterstützung

Browser	Version
Google Chrome	Letzte drei Hauptversionen
Mozilla Firefox	Letzte drei Hauptversionen
Microsoft Edge	Letzte drei Hauptversionen
Apple Safari für macOS	Letzte zwei Hauptversionen

Unterstützte AWS Regionen für AWS CloudShell

Dieser Abschnitt enthält die Liste der unterstützten AWS Regionen und Opt-in-Regionen für AWS CloudShell. Eine Liste der AWS Dienstendpunkte und Kontingente für CloudShell finden Sie AWS CloudShell auf der Seite im. Allgemeine Amazon Web Services-Referenz

Im Folgenden sind die unterstützten AWS Regionen aufgeführt für AWS CloudShell:

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

GovCloud Regionen

Im Folgenden sind die unterstützten GovCloud Regionen aufgeführt für CloudShell:

- AWS GovCloud (USA-Ost)

- AWS GovCloud (USA West)

Opt-In-Regionen

Opt-In-Region sind nicht standardmäßig aktiviert. Sie müssen diese Regionen manuell aktivieren, um sie verwenden zu können. Weitere Informationen finden Sie unter Verwaltung von AWS-Regionen. Im Folgenden sind die unterstützten Opt-in-Regionen aufgeführt für CloudShell:

- Afrika (Kapstadt)
- Asia Pacific (Hongkong)
- Asien-Pazifik (Jakarta)
- Europa (Milan)
- Naher Osten (Bahrain)
- Naher Osten (VAE)

Unterstützte Regionen für Docker

Die AWS CloudShell Rechenumgebung unterstützt nur Docker-Container in den folgenden Regionen:

- US East (Ohio)
- USA Ost (Nord-Virginia)
- USA West (Oregon)
- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Europe (Frankfurt)
- Europa (Irland)
- Europe (London)
- Europe (Paris)
- Südamerika (São Paulo)

Unterstützte Regionen für AWS CloudShell VPC

AWS CloudShell VPC-Umgebungen werden nur in den folgenden Regionen unterstützt:

- US East (Ohio)
- USA Ost (Nord-Virginia)
- USA West (Oregon)
- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Europe (Frankfurt)
- Europa (Irland)
- Europe (London)
- Europe (Paris)
- Südamerika (São Paulo)

Servicekontingente und Einschränkungen für AWS CloudShell

Auf dieser Seite werden die Servicekontingente und Einschränkungen beschrieben, die für die folgenden Bereiche gelten:

- Persistenter Speicher
- Monatliche Nutzung
- Größe des Befehls
- Gleichzeitige Shells
- Shell-Sitzungen
- Netzwerkzugriff und Datenübertragung
- Systemdateien und Neuladen von Seiten

Persistenter Speicher

Mit AWS CloudShell verfügen Sie kostenlos über einen dauerhaften Speicher von AWS-Region jeweils 1 GB. Der persistente Speicher befindet sich in Ihrem Home-Verzeichnis ($HOME) und ist für Sie privat. Im Gegensatz zu kurzlebigen Umgebungsressourcen, die nach dem Ende jeder Shell-Sitzung wiederverwendet werden, bleiben Daten in Ihrem Home-Verzeichnis zwischen den Sitzungen bestehen.

> **Note**
>
> CloudShell VPC-Umgebungen haben keinen persistenten Speicher. Das $HOME-Verzeichnis wird gelöscht, wenn Ihre VPC-Umgebung das Zeitlimit überschreitet (nach 20-30 Minuten Inaktivität) oder wenn Sie Ihre Umgebung löschen.

Wenn Sie die Verwendung von AWS CloudShell in beenden AWS-Region, werden die Daten nach dem Ende Ihrer letzten Sitzung 120 Tage lang im persistenten Speicher dieser Region aufbewahrt. Nach 120 Tagen werden Ihre Daten automatisch aus dem persistenten Speicher dieser Region gelöscht, sofern Sie keine Maßnahmen ergreifen. Sie können das Löschen verhindern, indem Sie in

dieser Datei AWS CloudShell erneut starten AWS-Region. Weitere Informationen finden Sie unter Schritt 2: Wählen Sie eine Region aus AWS CloudShell, starten Sie und wählen Sie eine Shell aus.

> **Note**
>
> Nutzungsszenario
> Márcia hat früher AWS CloudShell Dateien in ihren Heimatverzeichnissen in zwei Verzeichnissen gespeichert AWS-Regionen: USA Ost (Nord-Virginia) und Europa (Irland). Danach begann sie, die Software AWS CloudShell ausschließlich in Europa (Irland) zu verwenden, und stellte den Start von Shell-Sitzungen im Osten der USA (Nord-Virginia) ein. Vor Ablauf der Frist für das Löschen von Daten in USA Ost (Nord-Virginia) beschließt Márcia, die Wiederverwendung ihres Home-Verzeichnisses zu verhindern, indem sie erneut die Region USA Ost (Nord-Virginia) startet AWS CloudShell und auswählt. Da sie Europa (Irland) kontinuierlich für Shell-Sitzungen verwendet hat, ist ihr persistenter Speicher in dieser Region nicht betroffen.

Monatliche Nutzung

AWS CloudShell Für jede einzelne Person gibt es monatliche AWS-Region Nutzungskontingente AWS-Konto. Wenn Sie versuchen, darauf zuzugreifen, AWS CloudShell nachdem Sie das monatliche Kontingent für diese Region erreicht haben, wird eine Meldung angezeigt, in der erklärt wird, warum die Shell-Umgebung nicht gestartet werden kann.

> **Note**
>
> Wenn Sie Ihre monatlichen Nutzungskontingente erhöhen müssen, wenden Sie sich mit den folgenden Informationen an den AWS-Support:
>
> - CloudShell Nutzungsregion
> - Ihr Anwendungsfall. Zum Beispiel AWS CLI-Betrieb und Linux-Befehlsausführung
> - Die Anzahl der CloudShell Benutzer. Zum Beispiel 5-10
> - Die maximale geschätzte Zeit, die Sie CloudShell in der Region verwenden
>
> Wir können eine Erhöhung der geschätzten Höchstzeit von 200 Stunden auf 1000 Stunden pro Monat genehmigen.

Größe des Befehls

Die Befehlsgröße darf 65412 Zeichen nicht überschreiten.

> **Note**
>
> Wenn Sie den Befehl ausführen möchten, der mehr als 65412 Zeichen enthält, erstellen Sie ein Skript mit der Sprache Ihrer Wahl und führen Sie es dann über die Befehlszeilenschnittstelle aus. Weitere Informationen zu den verschiedenen vorinstallierten Programmen, auf die über die Befehlszeilenschnittstelle zugegriffen werden kann, finden Sie unter Vorinstallierte Software.
> Ein Beispiel dafür, wie Sie ein Skript erstellen und es dann über die Befehlszeilenschnittstelle ausführen, finden Sie unter Tutorial: Erste Schritte mit. AWS CloudShell

Gleichzeitige Shells

- Gleichzeitige Shells: Sie können AWS-Region für Ihr Konto jeweils bis zu 10 Shells gleichzeitig ausführen.

Shell-Sitzungen

- Inaktive Sitzungen: AWS CloudShell ist eine interaktive Shell-Umgebung. Wenn Sie 20—30 Minuten lang nicht mit der Tastatur oder dem Mauszeiger mit ihr interagieren, wird Ihre Shell-Sitzung beendet. Laufende Prozesse zählen nicht als Interaktionen.
- Sitzungen mit langer Laufzeit: Eine Shell-Sitzung, die etwa 12 Stunden ununterbrochen läuft, wird automatisch beendet, auch wenn der Benutzer während dieses Zeitraums regelmäßig mit ihr interagiert.

Netzwerkzugriff und Datenübertragung

Die folgenden Einschränkungen gelten sowohl für den eingehenden als auch für den ausgehenden Datenverkehr in Ihrer AWS CloudShell Umgebung:

- Ausgehend: Sie können auf das öffentliche Internet zugreifen.

- Eingehend: Sie können nicht auf eingehende Ports zugreifen. Es ist keine öffentliche IP-Adresse verfügbar.

> **Warning**
>
> Beim Zugriff auf das öffentliche Internet besteht das Risiko, dass bestimmte Benutzer Daten aus der AWS CloudShell Umgebung exportieren. Wir empfehlen, dass IAM-Administratoren die Liste der zugelassenen AWS CloudShell Benutzer mithilfe der IAM-Tools verwalten. Informationen darüber, wie bestimmten Benutzern der Zugriff explizit verweigert werden kann, finden Sie unter. Verwaltung zulässiger Aktionen mithilfe benutzerdefinierter Richtlinien AWS CloudShell

Datenübertragung: Das Hoch- und Herunterladen von Dateien zu und von großen Dateien AWS CloudShell kann langsam sein. Alternativ können Sie Dateien von einem Amazon S3 S3-Bucket über die Befehlszeilenschnittstelle der Shell in Ihre Umgebung übertragen.

Einschränkungen bei Systemdateien und beim erneuten Laden von Seiten

- Systemdateien: Wenn Sie Dateien, die für die Rechenumgebung erforderlich sind, falsch ändern, können Probleme beim Zugriff auf oder bei der Verwendung der AWS CloudShell Umgebung auftreten. In diesem Fall müssen Sie möglicherweise Ihr Home-Verzeichnis löschen, um wieder Zugriff darauf zu haben.
- Seiten neu laden: Um die AWS CloudShell Benutzeroberfläche neu zu laden, verwenden Sie die Schaltfläche „Aktualisieren“ in Ihrem Browser anstelle der Standardtastenkombination für Ihr Betriebssystem.

Dokumentenverlauf für das AWS CloudShell Benutzerhandbuch

Neueste Aktualisierungen

In der folgenden Tabelle werden wichtige Änderungen am AWS CloudShell Benutzerhandbuch beschrieben.

Änderung	Beschreibung	Datum
Amazon VPC-Unterstützung für AWS CloudShell bestimmte Regionen	Unterstützung für die Erstellung und Verwendung von AWS CloudShell VPC-Umgebungen in bestimmten Regionen hinzugefügt.	13. Juni 2024
Dem AWS CloudShell Benutzerhandbuch wurden neue Tutorials hinzugefügt	Es wurden zwei neue Tutorials hinzugefügt, in denen beschrieben wird, wie ein Docker-Container erstellt AWS CloudShell und in ein Amazon ECR-Repository übertragen wird und wie eine Lambda-Funktion über bereitgestellt wird. AWS CDK	27. Dezember 2023
Docker-Container werden in bestimmten Regionen unterstützt AWS CloudShell	Support für Docker-Container mit AWS CloudShell wurde in bestimmten Regionen hinzugefügt.	27. Dezember 2023
AWS CloudShell wurde migriert, um jetzt Amazon Linux 2023 (AL2023) zu verwenden	AWS CloudShell verwendet jetzt AL2023 und wurde von Amazon Linux 2 migriert.	4. Dezember 2023

Neue AWS-Regionen für AWS CloudShell	AWS CloudShell ist jetzt in den folgenden AWS Regionen allgemein verfügbar: • USA West (Nordkalifornien) • Afrika (Kapstadt) • Asia Pacific (Hongkong) • Asien-Pazifik (Osaka) • Asien-Pazifik (Seoul) • Asien-Pazifik (Jakarta) • Asien-Pazifik (Singapur) • Europa (Paris) • Europe (Stockholm) • Europe (Milan) • Naher Osten (Bahrain) • Naher Osten (VAE)	16. Juni 2023
Starten Sie AWS CloudShell auf dem Console Toolbar	Starten Sie CloudShell auf derConsole Toolbar, unten links auf der Konsole, indem Sie CloudShell.	28. März 2023
Neue AWS Regionen für AWS CloudShell	AWS CloudShell ist jetzt in den folgenden AWS Regionen verfügbar: • Kanada (Zentral) • Europa (London) • Südamerika (São Paulo)	6. Oktober 2022
AWS CloudShell unterstützt in AWS in den USA GovCloud	AWS CloudShell wird jetzt in der AWS-Region GovCloud (USA) unterstützt.	29. Juni 2022

Häufig gestellte Fragen zur Sicherheit	Zusätzliche FAQs konzentrieren sich auf Sicherheitsfragen.	14. April 2022
Web-Sockets	Zu den Netzwerkanforderungen wurde ein Abschnitt hinzugefügt, in dem die Verwendung CloudShell des WebSocket Protokolls erklärt wird.	21. März 2022
Problembehandlung mit den Pfeiltasten in PowerShell	Folgen Sie den Anweisungen, um die Pfeiltasten zu reparieren, die beim Drücken falsch Buchstaben ausgeben.	7. Februar 2022
Automatische Vervollständigung der Tabulatortaste	Neue Dokumentation, die erklärt, wie die Bash-Vervollständigung verwendet wird, die die automatische Vervollständigung von teilweise eingegebenen Befehlen oder Argumenten durch Drücken der Tabulatortaste ermöglicht.	24. September 2021
Regionen angeben AWS	Dokumentation zur Angabe von Standardeinstellungen AWS-Region für AWS CLI Befehle.	11. Mai 2021
Formatierung in PDF- und Kindle-Versionen	Feste Bildgrößen und Text in Tabellenzellen.	10. März 2021

Version für allgemeine Verfügbarkeit (GA) von AWS CloudShell in ausgewählten AWS Regionen	AWS CloudShell ist jetzt in den folgenden AWS Regionen allgemein verfügbar: • US East (Ohio) • USA Ost (Nord-Virginia) • USA West (Oregon) • Asien-Pazifik (Tokio) • Europa (Irland) • Asien-Pazifik (Mumbai) • Asien-Pazifik (Sydney) • Europa (Frankfurt)	15. Dezember 2020

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.