Handbuch „Erste Schritte“

AWS-Managementkonsole

Version 1.0

AWS-Managementkonsole: Handbuch „Erste Schritte“

Table of Contents

Was ist der AWS-Managementkonsole?

Das AWS-Managementkonsoleist eine webbasierte Anwendung, die alle einzelnen AWS Servicekonsolen enthält und einen zentralen Zugriff darauf bietet. Sie können Unified Navigation verwenden, AWS-Managementkonsole um nach Diensten zu suchen, Benachrichtigungen anzuzeigen AWS CloudShell, auf Konto- und Rechnungsinformationen zuzugreifen und auf diese zuzugreifen und Ihre allgemeinen Konsoleneinstellungen anzupassen. Die Startseite von AWS-Managementkonsole heißt AWS Console Home. Von aus AWS Console Home können Sie Ihre AWS Anwendungen verwalten und auf alle anderen einzelnen Servicekonsolen zugreifen. Mithilfe von Widgets können Sie auch anpassen AWS Console Home , dass weitere hilfreiche Informationen über AWS und Ihre Ressourcen angezeigt werden. Sie können Widgets wie „Zuletzt besucht“, „AWS Health“ und mehr hinzufügen, entfernen und neu anordnen.

Themen

Funktionen von AWS-Managementkonsole

AWS-Managementkonsole Zu den wichtigen Merkmalen von gehören die folgenden:

- Zu den AWS Servicekonsolen navigieren — Sie können Unified Navigation verwenden, um auf kürzlich besuchte Servicekonsolen zuzugreifen, Dienste anzuzeigen und zu Ihrer Favoritenliste hinzuzufügen, auf Ihre Konsoleneinstellungen zuzugreifen und darauf zuzugreifen AWS-Benutzerbenachrichtigungen.
- Suchen Sie nach AWS Diensten und anderen AWS Informationen — Verwenden Sie Unified Search, um nach AWS Diensten und Funktionen sowie AWS Marktprodukten zu suchen.
- Passen Sie die Konsole an — Mithilfe der vereinheitlichten Einstellungen können Sie verschiedene Aspekte von anpassen AWS-Managementkonsole. Dazu gehören die Sprache, die Standardregion und mehr.
- CLI-Befehle ausführen — AWS CloudShell ist direkt von der Konsole aus zugänglich. Sie können CloudShell es verwenden, um AWS CLI-Befehle für Ihre bevorzugten Dienste auszuführen.

- Auf alle AWS Ereignisbenachrichtigungen zugreifen — Sie können den verwenden AWS-Managementkonsole , um auf Benachrichtigungen von AWS-Benutzerbenachrichtigungen und zuzugreifen AWS Health.
- Anpassen AWS Console Home — Mithilfe von Widgets können Sie Ihr AWS Console Home Erlebnis vollständig anpassen.
- AWS Anwendungen erstellen und verwalten — Verwalten und überwachen Sie die Kosten, den Zustand, den Sicherheitsstatus und die Leistung Ihrer Anwendungen mithilfe von MyApplications in AWS Console Home.
- Chatten Sie mit Amazon Q — Sie können direkt von der Konsole aus Antworten auf Ihre AWS-Service Fragen mit generativer künstlicher Intelligenz (KI) erhalten. Sie können sich auch mit einem Live-Agenten in Verbindung setzen, um zusätzlichen Support zu erhalten.
- Steuern Sie den AWS Kontozugriff in Ihrem Netzwerk — Sie können AWS-Managementkonsole Private Access verwenden, AWS-Managementkonsole um den Zugriff auf bestimmte bekannte AWS Konten zu beschränken, wenn der Datenverkehr aus Ihrem Netzwerk stammt.

Einzelne AWS Servicekonsolen im AWS-Managementkonsole

Jeder AWS Dienst verfügt über eine eigene Servicekonsole, auf die Sie innerhalb der zugreifen können AWS-Managementkonsole. Einstellungen, die Sie in den vereinheitlichten Einstellungen für auswählen AWS-Managementkonsole, wie z. B. Grafikmodus und Standardsprache, werden auf alle einzelnen AWS Konsolen angewendet. AWS Servicekonsolen bieten eine breite Palette von Tools für Cloud-Computing sowie Informationen zu Ihrem Konto und zu Ihrer Abrechnung. Wenn Sie mehr über einen bestimmten Service und seine Konsole erfahren möchten, zum Beispiel Amazon Elastic Compute Cloud, navigieren Sie mit Unified Search in der AWS-Managementkonsole Navigationsleiste zu der entsprechenden Konsole und greifen Sie von der Dokumentationswebsite auf die EC2 AWS Amazon-Dokumentation zu.

Wenn Sie zur Konsole eines einzelnen AWS Dienstes navigieren, können Sie weiterhin oben in der Konsole auf Funktionen zur AWS-Managementkonsole Verwendung von Unified Navigation zugreifen. Sie können Feedback für die Konsole eines einzelnen Dienstes hinterlassen, indem Sie zu dieser Konsole navigieren und in der Fußzeile der Seite Feedback auswählen.

Zugreifen auf AWS-Managementkonsole

Sie können auf die AWS-Managementkonsole unter https://console.aws.amazon.com/zugreifen.

Zugriff auf die AWS-Managementkonsole mit Mobilgeräten

Das AWS-Managementkonsoleist so konzipiert, dass es sowohl auf Tablets als auch auf anderen Arten von Mobilgeräten funktioniert:

- Der horizontale und vertikale Anzeigeplatz wurden maximiert, damit mehr Inhalte auf dem Bildschirm angezeigt werden können.
- Für eine optimierte Touch-Umgebung wurden Schaltflächen und Auswahlen vergrößert.

Um AWS-Managementkonsole auf einem Mobilgerät auf das zuzugreifen, müssen Sie das verwenden AWS Console Mobile Application. Diese App ist für Android und iOS verfügbar. Die Console Mobile Application bietet Aufgaben, die für Mobilgeräte relevant sind und eine gute Ergänzung zum vollständigen Weberlebnis sind. Sie können beispielsweise Ihre bestehenden EC2 Amazon-Instances und CloudWatch Amazon-Alarme ganz einfach von Ihrem Telefon aus einsehen und verwalten. Weitere Informationen finden Sie unter Was ist der AWS Console Mobile Application? im AWS Console Mobile Application Benutzerhandbuch.

Sie können die Console Mobile Application von Amazon Appstore, Google Play und dem iOS App Store herunterladen.

Erste Schritte mit einem Dienst in der AWS-Managementkonsole

Die AWS-Managementkonsole bietet mehrere Methoden für die Navigation zu einzelnen Servicekonsolen.

So öffnen Sie eine Konsole für einen Service

Führen Sie eine der folgenden Aktionen aus:

- Geben Sie in das Suchfeld in der Navigationsleiste den Namen des Services ganz oder teilweise ein. Wählen Sie dann unter Services den gewünschten Service in der Liste der Suchergebnisse aus. Weitere Informationen finden Sie unter Suchen Sie mit Unified Search nach Produkten, Dienstleistungen, Funktionen und mehr in der AWS-Managementkonsole.
- Unter Recently visited services (Kürzlich besuchte Services) wählen Sie einen Servicenamen aus.
- Wählen Sie im Widget Kürzlich besuchte Dienste die Option Alle AWS Dienste anzeigen aus. Wählen Sie dann auf der Seite Alle AWS Dienste einen Dienstnamen aus.
- Wählen Sie in der Navigationsleiste Services aus, um eine vollständige Liste der Services zu öffnen. Wählen Sie unter Kürzliche besuchte Services oder Alle Services einen Servicenamen aus.

Verwenden der AWS-Managementkonsole Navigationsleiste über Unified Navigation

In diesem Thema wird beschrieben, wie Unified Navigation verwendet wird. Unified Navigation bezieht sich auf die Navigationsleiste, die als Kopf- und Fußzeile der Konsole fungiert. Sie können Unified Navigation verwenden, um:

- Suchen Sie nach AWS Diensten, Funktionen, Produkten und mehr und greifen Sie darauf zu.
- Starten Sie AWS Cloudshell.
- Greifen AWS Sie auf Benachrichtigungen und AWS Gesundheitsereignisse zu.
- Holen Sie sich Unterstützung aus einer Vielzahl von AWS Wissensquellen.
- Konfigurieren Sie das, AWS-Managementkonsole indem Sie Ihre Standardsprache, den visuellen Modus, die Region und mehr auswählen.
- Greifen Sie auf Konto-, Organisations-, Servicekontingent- und Rechnungsinformationen zu.

Themen

Zugriff auf das Menü „Dienste“ im AWS-Managementkonsole

Sie können das Menü Dienste neben der Suchleiste verwenden, um auf Ihre zuletzt besuchten Dienste zuzugreifen, Ihre Favoritenliste einzusehen und alle AWS Dienste anzusehen. Sie können

Dienste auch nach Typ anzeigen, indem Sie einen Diensttyp auswählen, z. B. Analytics oder Anwendungsintegration.

Im folgenden Verfahren wird beschrieben, wie Sie auf das Menü Dienste zugreifen.

So greifen Sie auf das Menü „Dienste“ zu

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Wählen Sie in der Navigationsleiste „Dienste“ („Dienste“).
3. (Optional) Wählen Sie Zuletzt besucht, um Dienste und Anwendungen anzuzeigen, mit denen Sie kürzlich interagiert haben.
4. (Optional) Wählen Sie „Favoriten“, um Ihre Favoritenliste anzuzeigen.
5. (Optional) Wählen Sie Alle Anwendungen aus, um Ihre MyApplications-Anwendungen anzuzeigen.
6. (Optional) Wählen Sie Alle Dienste aus, um eine alphabetische Liste aller AWS Dienste anzuzeigen.
7. (Optional) Wählen Sie einen Diensttyp aus, um AWS Dienste nach Typ anzuzeigen.

Suchen Sie mit Unified Search nach Produkten, Dienstleistungen, Funktionen und mehr in der AWS-Managementkonsole

Das Suchfeld in der Navigationsleiste bietet ein einheitliches Suchwerkzeug für die Suche nach AWS Diensten und Funktionen, Servicedokumentationen, AWS Marketplace Produkten und mehr. Geben Sie einfach ein paar Zeichen oder eine Frage ein, um Ergebnisse aus allen verfügbaren Inhaltstypen zu generieren. Jedes Wort, das Sie eingeben, verfeinert Ihre Ergebnisse weiter. Zu den verfügbaren Inhaltstypen gehören:

- Dienstleistungen
- Features
- Dokumente
- Blogs
- Knowledge-Artikel
- Ereignisse
- Lernprogramme

- Marketplace
- Ressourcen

> **Note**
>
> Sie können Ihre Suchergebnisse so filtern, dass nur Ressourcen angezeigt werden, indem Sie eine gezielte Suche durchführen. Um eine gezielte Suche durchzuführen, geben Sie `/Resources` zu Beginn Ihrer Anfrage in die Suchleiste ein und wählen Sie im Dropdownmenü /Resources aus. Geben Sie dann den Rest Ihrer Anfrage ein.

Themen

Auf der Suche nach AWS Produkten in der AWS-Managementkonsole

Das folgende Verfahren beschreibt, wie Sie mit der Suchfunktion nach AWS Produkten suchen.

So suchen Sie nach einem Service, einer Funktion, einer Dokumentation oder einem AWS Marketplace Produkt

1. Geben Sie in das Suchfeld in der AWS-ManagementkonsoleNavigationsleiste von Ihre Anfrage ein.
2. Wählen Sie einen beliebigen Link, um zu Ihrem gewünschten Ziel zu gelangen.

> **Tip**
>
> Sie können auch Ihre Tastatur verwenden, um schnell zum obersten Suchergebnis zu navigieren. Drücken Sie zuerst Alt+S (Windows) oder Option+S (macOS), um auf die Suchleiste zuzugreifen. Beginnen Sie dann mit der Eingabe Ihres Suchbegriffs. Drücken Sie die Eingabetaste, wenn das gewünschte Ergebnis am Anfang der Liste angezeigt wird. Geben Sie beispielsweise ec2 ein und drücken Sie die Eingabetaste, um schnell zu Amazon EC2-Konsole zu navigieren.

Verfeinern Sie Ihre Suche im AWS-Managementkonsole

Sie können Ihre Suche nach Inhaltstyp verfeinern und zusätzliche Informationen zu Suchergebnissen anzeigen.

Um Ihre Suche auf einen bestimmten Inhaltstyp zu verfeinern

1. Geben Sie in das Suchfeld in der AWS-ManagementkonsoleNavigationsleiste von Ihre Anfrage ein.
2. Wählen Sie einen der Inhaltstypen neben Ihren Suchergebnissen aus.
3. (Optional) Um alle Ergebnisse für eine bestimmte Kategorie zu sehen:
   - Wählen Sie Mehr anzeigen. Es öffnet sich ein neuer Tab mit den Ergebnissen.
4. (Optional) Um zusätzliche Informationen zu Ihren Suchergebnissen anzuzeigen:
   a. Bewegen Sie den Mauszeiger in den Suchergebnissen über ein Suchergebnis.
   b. Sehen Sie sich die verfügbaren zusätzlichen Informationen an.

Funktionen eines Dienstes anzeigen in der AWS-Managementkonsole

Sie können die Funktionen eines Dienstes in Ihren Suchergebnissen anzeigen.

Um die Funktionen eines Dienstes anzuzeigen

1. Geben Sie in das Suchfeld in der AWS-ManagementkonsoleNavigationsleiste von Ihre Anfrage ein.
2. Bewegen Sie den Mauszeiger in den Suchergebnissen unter Dienste über einen Dienst.
3. Wählen Sie einen der Links unter Top-Features aus.

Starten AWS CloudShell über die Navigationsleiste im AWS-Managementkonsole

AWS CloudShell ist eine browserbasierte, vorauthentifizierte Shell, die Sie direkt von der Navigationsleiste aus starten können. AWS-Managementkonsole Sie können AWS CLI Befehle für Dienste mit Ihrer bevorzugten Shell (Bash- oder Z-Shell) ausführen. PowerShell

Sie können CloudShell von der aus AWS-Managementkonsole mit einer der folgenden beiden Methoden starten:

- Wählen Sie das CloudShell Symbol in der Fußzeile der Konsole.
- Wählen Sie das CloudShell Symbol in der Navigationsleiste der Konsole.

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

Informationen darüber, AWS-Regionen wo verfügbar AWS CloudShell ist, finden Sie in der Liste der AWS regionalen Dienste. Die Auswahl der Konsolenregion ist mit der CloudShell Region synchronisiert. Wenn es in einer ausgewählten Region nicht CloudShell verfügbar ist, CloudShell funktioniert es in der nächstgelegenen Region.

Zugreifen auf AWS Benachrichtigungen und Gesundheitsereignisse

Über die Navigationsleiste können Sie auf einige Ihrer AWS Benachrichtigungen zugreifen und Gesundheitsereignisse einsehen. Du kannst auch über AWS-Benutzerbenachrichtigungen die Navigationsleiste auf all deine AWS Benachrichtigungen und das AWS Health Dashboard zugreifen.

Weitere Informationen findest du unter Was ist AWS-Benutzerbenachrichtigungen? im AWS-Benutzerbenachrichtigungen Benutzerhandbuch und Was ist AWS Health? im AWS Health Benutzerhandbuch

Das folgende Verfahren beschreibt, wie Sie auf Ihre AWS Veranstaltungsinformationen zugreifen können.

So greifen Sie auf Ihre AWS Veranstaltungsinformationen zu

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Wählen Sie in der Navigationsleiste das Glockensymbol aus.
3. Sehen Sie sich Ihre Benachrichtigungen und Gesundheitsereignisse an.
4. (Optional) Wähle „Alle Benachrichtigungen anzeigen“, um zur Benutzerbenachrichtigungen Konsole zu gelangen.
5. (Optional) Wählen Sie „Alle Gesundheitsereignisse anzeigen“, um zur AWS Health Konsole zu navigieren.

Supportanfragen

Sie können Unterstützung erhalten, indem Sie das Fragezeichensymbol in der Navigationsleiste auswählen. Im Support-Menü können Sie Folgendes wählen:

- Navigieren Sie zur Support Center-Servicekonsole
- Holen Sie sich kompetente Hilfe von AWS IQ
- Sehen Sie sich kuratiertes Wissen aus Community-Artikeln und dem Knowledge Center auf re:POST an AWS
- Gehe zur Dokumentation AWS
- Navigiere zu den AWS Schulungen
- Navigieren Sie zum Resource Center für die ersten AWS Schritte
- Hinterlassen Sie Feedback zu allen Servicekonsolen, auf die Sie gerade zugreifen

> **Note**
>
> Sie können dies auch tun, indem Sie in der Fußzeile der Konsole Feedback auswählen. Der Titel des sich öffnenden Modals zeigt, für welche Konsole du gerade Feedback abgibst

Du kannst auch jederzeit in der Konsole Hilfe erhalten, dich mit einem Live-Agenten verbinden und Fragen stellen, AWS indem du mit AWS Q chattest. Weitere Informationen finden Sie unter ???.

Konfiguration der AWS-Managementkonsole Verwendung von Unified Settings

In diesem Thema wird beschrieben, wie Sie AWS-Managementkonsole mithilfe der Seite „Vereinheitlichte Einstellungen“ Einstellungen konfigurieren, die für alle Servicekonsolen gelten.

Themen

Konfiguration einheitlicher Einstellungen in der AWS-Managementkonsole

Sie können Einstellungen und Standardeinstellungen wie Anzeige, Sprache und Region auf der Seite AWS-Managementkonsole Vereinheitlichte Einstellungen konfigurieren. Sie können über die Navigationsleiste in Unified Navigation auf Unified Settings zugreifen. Der visuelle Modus und die Standardsprache können auch direkt über die Navigationsleiste eingestellt werden. Diese Änderungen gelten für alle Servicekonsolen.

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

Themen

Zugriff auf die vereinheitlichten Einstellungen in der AWS-Managementkonsole

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

So greifen Sie auf die einheitlichen Einstellungen zu:

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Wählen Sie in der Navigationsleiste das Zahnradsymbol (#) aus.

3. Um die Seite mit den vereinheitlichten Einstellungen zu öffnen, wählen Sie Alle Benutzereinstellungen anzeigen.

Zurücksetzen der vereinheitlichten Einstellungen in der AWS-Managementkonsole

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

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

Um alle vereinheitlichten Einstellungen zurückzusetzen

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Wählen Sie in der Navigationsleiste das Zahnradsymbol (#).
3. Öffnen Sie die Seite „Vereinheitlichte Einstellungen“, indem Sie Alle Benutzereinstellungen anzeigen wählen.
4. Wählen Sie Alle zurücksetzen.

Bearbeiten einheitlicher Einstellungen in der AWS-Managementkonsole

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

Um vereinheitlichte Einstellungen zu bearbeiten

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Wählen Sie in der Navigationsleiste das Zahnradsymbol (#).
3. Öffnen Sie die Seite „Vereinheitlichte Einstellungen“, indem Sie Alle Benutzereinstellungen anzeigen wählen.
4. Klicken Sie auf Bearbeiten neben den gewünschten Einstellungen:

    - Lokalisierung und Standardregion:

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

  Weitere Informationen zum Regionen-Routing in der AWS-Managementkonsole finden Sie unter Auswahl einer Region.

- Anzeige:
  - Unter Visual Mode (Visueller Modus) können Sie Ihre Konsole auf den Hell- oder den Dunkelmodus oder auf den Standardanzeigemodus des Browsers einstellen.

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

5. Wählen Sie Änderungen speichern aus.

Ändern des visuellen Modus des AWS-Managementkonsole

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

So ändern Sie den visuellen Modus über die Navigationsleiste

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

Wählen Sie Ihre Region

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

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

Themen

Wählen Sie eine Region aus der Navigationsleiste im AWS-Managementkonsole

Das folgende Verfahren beschreibt, wie Sie Ihre Region über die Navigationsleiste ändern können.

Um eine Region aus der Navigationsleiste auszuwählen

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Wählen Sie auf der Navigationsleiste den Namen der aktuell angezeigten Region aus.
3. Wählen Sie eine Region aus, zu der Sie wechseln möchten.

Einstellung der Standardregion im AWS-Managementkonsole

Im folgenden Verfahren wird beschrieben, wie Sie Ihre Standardregion auf der Seite „Vereinheitlichte Einstellungen“ ändern können.

So legen Sie Ihre Standardregion fest

1. Wählen Sie in der Navigationsleiste das Zahnradsymbol (#).

2. Wählen Sie Alle Benutzereinstellungen anzeigen aus, um zur Seite „Vereinheitlichte Einstellungen“ zu gelangen.
3. Wählen Sie Bearbeiten neben Lokalisierung und Standardregion aus.
4. Wählen Sie unter Standardregion eine Region aus.

> **Note**
>
> Wenn Sie keine Standardregion auswählen, ist die letzte Region, die Sie aufgerufen haben, die Standardregion.

5. Wählen Sie Save settings (Einstellungen speichern).
6. (Optional) Wählen Sie Gehe zu neuer Standardregion, um sofort zu Ihrer neuen Standardregion zu wechseln.

Favoriten im AWS-Managementkonsole

Um schneller auf Ihre häufig verwendeten Dienste und Anwendungen zuzugreifen, können Sie deren Servicekonsolen in einer Favoritenliste speichern. Mit dem können Sie Favoriten hinzufügen und entfernen AWS-Managementkonsole. Wenn Sie einen Dienst oder eine Anwendung zu Ihren Favoriten hinzufügen, wird sie in der Favoriten-Schnellleiste angezeigt.

Themen

- Hinzufügen von Favoriten in der AWS-Managementkonsole
- Zugreifen auf Favoriten in der AWS-Managementkonsole
- Entfernen von Favoriten in der AWS-Managementkonsole

Hinzufügen von Favoriten in der AWS-Managementkonsole

Sie können Dienste und Anwendungen über das Menü Dienste und das Menü Zuletzt besucht zu Ihren Favoriten hinzufügen. Sie können Dienste auch zu Ihren Favoriten hinzufügen, indem Sie die Suchergebnisseite im Suchfeld verwenden. Dienste und Anwendungen, die Sie zu Ihren Favoriten hinzufügen, werden in der Favoriten-Schnellleiste angezeigt.

Themen

- Favoriten-Schnellleiste in der AWS-Managementkonsole
- Hinzufügen von Diensten zu Ihren Favoriten im AWS-Managementkonsole

- Hinzufügen von Anwendungen zu Ihren Favoriten im AWS-Managementkonsole

Favoriten-Schnellleiste in der AWS-Managementkonsole

Die Favoriten-Schnellleiste wird angezeigt, wenn Sie mindestens einen AWS Dienst oder eine Anwendung zu Ihren Favoriten hinzugefügt haben. Die Favoriten-Schnellleiste befindet sich hinter der Navigationsleiste und ist in allen AWS Servicekonsolen sichtbar, sodass Sie schnell auf Ihre bevorzugten Dienste und Anwendungen zugreifen können. Sie können die Reihenfolge der Dienste und Anwendungen in der Favoriten-Schnellleiste neu anordnen, indem Sie einen Dienst oder eine Anwendung nach links oder rechts ziehen.

Hinzufügen von Diensten zu Ihren Favoriten im AWS-Managementkonsole

Sie können Dienste über das Menü Dienste oder über die Suchergebnisseite über das Suchfeld zu Ihren Favoriten hinzufügen.

Services menu

So fügen Sie Favoriten aus dem Menü „Dienste“ hinzu

1. Öffnen Sie die AWS-Managementkonsole.
2. Wählen Sie in der Navigationsleiste „Dienste“ („Dienste“) aus.
3. (Optional) Fügen Sie einen kürzlich besuchten Dienst zu Ihren Favoriten hinzu:
    a. Bewegen Sie den Mauszeiger unter Zuletzt besucht über einen Dienst.
    b. Wählen Sie den Stern neben dem Namen des Dienstes aus.
4. Wählen Sie Alle Dienste aus.
5. Bewegen Sie den Mauszeiger über den ausgewählten Dienst.
6. Wählen Sie den Stern neben dem Namen des Dienstes aus.

Search box

Um Favoriten aus dem Suchfeld hinzuzufügen

1. Öffnen Sie die AWS-Managementkonsole.
2. Geben Sie den Namen eines Dienstes in das Suchfeld ein.
3. Wählen Sie auf der Suchergebnisseite den Stern neben dem Namen des Dienstes aus.

> **Note**
>
> Nachdem Sie einen Dienst zu Ihren Favoriten hinzugefügt haben, wird er der Favoriten-Schnellleiste hinzugefügt, die der Navigationsleiste folgt.

Hinzufügen von Anwendungen zu Ihren Favoriten im AWS-Managementkonsole

Sie können Anwendungen über das Menü Dienste zu Ihren Favoriten hinzufügen.

Um Favoriten aus dem Menü Dienste hinzuzufügen

1. Öffnen Sie die AWS-Managementkonsole.
2. Wählen Sie in der Navigationsleiste „Dienste“ („Dienste“) aus.
3. (Optional) Fügen Sie eine kürzlich besuchte Anwendung zu Ihren Favoriten hinzu:
    a. Bewegen Sie den Mauszeiger unter Zuletzt besucht über eine Anwendung.
    b. Wählen Sie den Stern neben dem Namen der Anwendung aus.
4. Wählen Sie Applications (Anwendungen).
5. Bewegen Sie den Mauszeiger über die von Ihnen gewählte Anwendung.
6. Wählen Sie den Stern neben dem Namen der Anwendung aus.

> **Note**
>
> Nachdem Sie eine Anwendung zu Ihren Favoriten hinzugefügt haben, wird sie der Favoriten-Schnellleiste hinzugefügt, die der Navigationsleiste folgt.

Zugreifen auf Favoriten in der AWS-Managementkonsole

Sie können über das Menü Dienste, die Favoriten-Schnellleiste und das Favoriten-Widget auf Dienste und Anwendungen zugreifen, die zu Ihren Favoriten hinzugefügt wurden.

Services menu

So greifen Sie über das Menü „Dienste“ auf Ihre Favoriten zu

1. Öffnen Sie die AWS-Managementkonsole.

2. Wählen Sie in der Navigationsleiste „Dienste“ („Dienste“) aus.
3. Wählen Sie Favoriten.
4. Sehen Sie sich die Dienste und Anwendungen an, die Sie zu Ihren Favoriten hinzugefügt haben.
5. (Optional) Anwendungsressourcen anzeigen:
    a. Wählen Sie eine Anwendung aus.
    b. (Optional) Wählen Sie eine Ansicht aus.
    c. Sehen Sie sich Ihre Ressourcen an.
    d. (Optional) Wählen Sie einen Filter aus. Sie können Ihre Ressourcen nach Eigenschaften oder nach Tags filtern. Weitere Informationen finden Sie im AWS Resource Explorer Benutzerhandbuch unter Syntaxreferenz für Suchabfragen für Resource Explorer.
    e. (Optional) Wählen Sie eine Ressource aus, um sie in der entsprechenden Servicekonsole anzuzeigen.

> **Tip**
>
> Sie können dort weiter nach Ressourcen suchen, wo Sie aufgehört haben, indem Sie Dienste () wählen. Ihre angewendeten Suchfilter bleiben ebenfalls bestehen.

Favorites quickbar

Um über die Favoriten-Schnellleiste auf Ihre Favoriten zuzugreifen

1. Öffnen Sie die AWS-Managementkonsole.
2. Sehen Sie sich die Dienste und Anwendungen in der Favoriten-Schnellleiste an.

Favorites widget

So greifen Sie über das Favoriten-Widget auf Ihre Favoriten zu

1. Öffnen Sie die AWS-Managementkonsole.
2. (Optional) Fügen Sie das Favoriten-Widget hinzu, falls Sie es noch nicht haben:
    a. Wählen Sie auf der Startseite der Konsole die Schaltfläche + Widgets hinzufügen.

b. Ziehen Sie im Menü „Widgets hinzufügen“ das Favoriten-Widget mithilfe des Symbols und platzieren Sie es auf der Startseite Ihrer Konsole.

3. Sehen Sie sich die Dienste und Anwendungen im Favoriten-Widget an.

Weitere Informationen zu Widgets finden Sie unterthe section called “Arbeiten mit Widgets”.

Entfernen von Favoriten in der AWS-Managementkonsole

Sie können Dienste und Anwendungen über das Menü Dienste aus Ihren Favoriten entfernen. Sie können Dienste auch über die Suchergebnisseite in der Suchleiste entfernen.

Services menu

Um Favoriten aus dem Menü „Dienste“ zu entfernen

1. Öffnen Sie die AWS-Managementkonsole.
2. Wählen Sie auf der Navigationsleiste Services aus.
3. Wählen Sie Favoriten.
4. Deaktivieren Sie den Stern neben dem Dienst oder der Anwendung.

Search box

> **Note**
>
> Derzeit können Sie Dienste nur über die Suchergebnisseite aus der Suchleiste entfernen.

Um Favoriten aus dem Suchfeld zu entfernen

1. Öffnen Sie die AWS-Managementkonsole.
2. Geben Sie den Namen eines Dienstes in das Suchfeld ein.
3. Deaktivieren Sie auf der Suchergebnisseite den Stern neben dem Namen des Dienstes.

Ändern Sie Ihr Passwort in der AWS-Managementkonsole

AWS-ManagementkonsoleAbhängig von Ihrem Benutzertyp und Ihren Berechtigungen können Sie Ihr Passwort möglicherweise unter ändern. Im folgenden Thema wird beschrieben, wie Sie Ihr Passwort für jeden Benutzertyp ändern können.

Themen

- Root-Benutzer in der AWS-Managementkonsole
- IAM-Benutzer in der AWS-Managementkonsole
- IAM Identity Center-Benutzer im AWS-Managementkonsole
- Föderierte Identitäten in der AWS-Managementkonsole

Root-Benutzer in der AWS-Managementkonsole

Root-Benutzer können ihre Passwörter direkt über die ändern AWS-Managementkonsole. Ein Root-Benutzer ist der Kontoinhaber mit vollständigem Zugriff auf alle AWS Dienste und Ressourcen. Sie sind der Root-Benutzer, wenn Sie das AWS Konto erstellt haben und sich mit Ihrer Root-Benutzer-E-Mail-Adresse und Ihrem Passwort anmelden. Weitere Informationen finden Sie unter AWS IAM Identity Center Root-Benutzer im Benutzerhandbuch.

So ändern Sie Ihr Passwort als Root-Benutzer

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

   Das neue Passwort muss mindestens acht Zeichen enthalten, darunter:

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

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

IAM-Benutzer in der AWS-Managementkonsole

IAM-Benutzer können ihr Passwort AWS-Managementkonsole je nach ihren Berechtigungen unter ändern. Andernfalls müssen sie ein AWS Zugriffsportal verwenden. Ein IAM-Benutzer ist eine Identität in Ihrem AWS Konto, der bestimmte benutzerdefinierte Berechtigungen gewährt wurden. Sie sind ein IAM-Benutzer, wenn Sie das AWS Konto nicht erstellt haben und Ihr Administrator oder Helpdesk-Mitarbeiter Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt hat, die eine AWS Konto-ID oder einen Kontoalias, einen IAM-Benutzernamen und ein Passwort enthalten. Weitere Informationen finden Sie unter IAM-Benutzer im Benutzerhandbuch.AWS-Anmeldung

Wenn Sie über Berechtigungen gemäß der folgenden Richtlinie verfügen AWS: Erlaubt IAM-Benutzern, ihr eigenes Konsolenkennwort auf der Seite Sicherheitsanmeldedaten zu ändern, können Sie Ihr Passwort von der Konsole aus ändern. Weitere Informationen finden Sie im Benutzerhandbuch unter So ändert ein IAM-Benutzer sein eigenes Passwort.AWS Identity and Access Management

Falls Sie nicht über die erforderlichen Rechte zum Ändern Ihres Kennworts verfügen, AWS-Managementkonsole finden Sie im Benutzerhandbuch unter Zurücksetzen Ihres AWS IAM Identity Center Benutzerpassworts weitere Informationen.AWS IAM Identity Center

IAM Identity Center-Benutzer im AWS-Managementkonsole

AWS IAM Identity Center Benutzer müssen ihr Passwort über ein AWS Zugangsportal ändern. Weitere Informationen finden Sie im Benutzerhandbuch unter Zurücksetzen Ihres AWS IAM Identity Center Benutzerkennworts.AWS IAM Identity Center

Ein IAM Identity Center-Benutzer ist ein Benutzer, dessen AWS Konto Teil davon ist AWS Organizations , der sich über das AWS Zugriffsportal mit einer eindeutigen URL anmeldet. Diese Benutzer können entweder direkt in den Benutzern in IAM Identity Center oder in Active Directory oder einem anderen externen Identitätsanbieter erstellt werden. Weitere Informationen finden Sie unter AWS IAM Identity Center Benutzer im AWS-Anmeldung Benutzerhandbuch.

Föderierte Identitäten in der AWS-Managementkonsole

Benutzer von Federated Identity müssen ihr Passwort über ein AWS Zugriffsportal ändern. Weitere Informationen finden Sie im Benutzerhandbuch unter Zurücksetzen Ihres AWS IAM Identity Center BenutzerkennwortsAWS IAM Identity Center .

Federated Identity-Benutzer melden sich mit einem externen Identitätsanbieter (IdP) an. Sie sind eine föderierte Identität, wenn Sie entweder:

- Greifen Sie mit Anmeldeinformationen von Drittanbietern wie Login with Amazon, Facebook oder Google auf Ihr AWS Konto oder Ihre Ressourcen zu.
- Verwenden Sie dieselben Anmeldeinformationen, um sich bei Unternehmenssystemen und AWS -diensten anzumelden, und Sie verwenden ein benutzerdefiniertes Unternehmensportal, um sich anzumelden. AWS

Weitere Informationen finden Sie unter Federated Identity im AWS-Anmeldung Benutzerhandbuch. .

Änderung der Sprache des AWS-Managementkonsole

Das AWS Console Home Erlebnis umfasst die Seite Unified Settings, auf der Sie die Standardsprache für AWS Dienste in der ändern können AWS-Managementkonsole. Sie können die Standardsprache auch schnell über das Einstellungsmenü in der Navigationsleiste ändern.

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

Themen

- Unterstützte Sprachen
- Ändern der Standardsprache über die Navigationsleiste im AWS-Managementkonsole
- Ändern Sie die Standardsprache über Unified Settings in der AWS-Managementkonsole

Unterstützte Sprachen

Die unterstützt AWS-Managementkonsole derzeit die folgenden Sprachen:

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

Ändern der Standardsprache über die Navigationsleiste im AWS-Managementkonsole

Das folgende Verfahren beschreibt, wie Sie Ihre Standardsprache direkt über die Navigationsleiste ändern können.

So ändern Sie die Standardsprache über die Navigationsleiste

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Wählen Sie in der Navigationsleiste das Zahnradsymbol (#).
3. Wählen Sie für Sprache entweder die Option Browser-Standard oder die bevorzugte Sprache aus der Dropdown-Liste aus.

Ändern Sie die Standardsprache über Unified Settings in der AWS-Managementkonsole

Im folgenden Verfahren wird beschrieben, wie Sie Ihre Standardsprache auf der Seite „Vereinheitlichte Einstellungen“ ändern können.

So ändern Sie die Standardsprache in „Einheitliche Einstellungen“

1. Melden Sie sich an der AWS-Managementkonsole an.

2. Wählen Sie in der Navigationsleiste das Zahnradsymbol (#).
3. Um die Seite mit den vereinheitlichten Einstellungen zu öffnen, wählen Sie Alle Benutzereinstellungen anzeigen.
4. In Unified Settings (Einheitliche Einstellungen), wählen Sie Edit (Bearbeiten) neben Localization and default Region (Lokalisierung und Standardregion) aus.
5. Um die Sprache auszuwählen, die für die Konsole verwendet werden soll, aktivieren Sie eine der folgenden Optionen:

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

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

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

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

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

Zugriff auf Ihr AWS Konto, Ihre Organisation, Ihr Servicekontingent und Ihre Rechnungsinformationen in der AWS-Managementkonsole

Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie von der Konsole aus auf Informationen zu Ihrem AWS Konto, Ihren Servicekontingenten, Ihrer Organisation und Ihren Rechnungsinformationen zugreifen.

> **Note**
>
> Sie bietet AWS-Managementkonsole nur Zugriff auf Konto-, Organisations-, Servicekontingent- und Abrechnungsinformationen. Diese Dienste haben ihre eigenen separaten Konsolen. Weitere Informationen finden Sie hier:

- Verwalte dein AWS Konto im AWS -Kontenverwaltung Referenzhandbuch.
- Was ist AWS Organizations? im AWS Organizations Benutzerhandbuch.
- Was sind Service Quotas? im Service Quotas User Guide.
- Verwenden der AWS Fakturierung und Kostenmanagement Startseite im AWS Billing User Guide.

> **Tip**
>
> Weitere Informationen zu diesen Themen erhalten Sie auch, indem Sie Amazon Q kontaktieren. Weitere Informationen finden Sie unter Chat mit Amazon Q Developer.

Themen

Zugriff auf Kontoinformationen im AWS-Managementkonsole

Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie von der Konsole aus auf Informationen zu Ihrem AWS Konto zugreifen.

Um auf Ihre Kontoinformationen zuzugreifen

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Wählen Sie auf der Navigationsleiste den Namen Ihres Kontos aus.
3. Wählen Sie Konto.
4. Sehen Sie sich Ihre Kontoinformationen an.

> **Note**
>
> Wenn Sie Ihr AWS Konto schließen möchten, finden Sie im AWS -Kontenverwaltung Referenzhandbuch weitere Informationen unter AWS Konto schließen.

Zugreifen auf Unternehmensinformationen im AWS-Managementkonsole

Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie über die Konsole auf Informationen zu Ihren AWS Organisationen zugreifen.

So greifen Sie auf Unternehmensinformationen zu

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Wählen Sie auf der Navigationsleiste den Namen Ihres Kontos aus.
3. Wählen Sie Organizations aus.
4. Sehen Sie sich Ihre Unternehmensinformationen an.

Zugreifen auf Informationen zum Servicekontingent im AWS-Managementkonsole

Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie über die Konsole auf Informationen zu Servicekontingenten zugreifen.

Um auf Informationen zu Servicekontingenten zuzugreifen

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Wählen Sie auf der Navigationsleiste den Namen Ihres Kontos aus.
3. Wählen Sie Service Quotas.
4. Informationen zu Ihren Servicekontingenten anzeigen und verwalten.

Zugriff auf Rechnungsinformationen in der AWS-Managementkonsole

Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie von der Konsole aus auf Informationen zu Ihren AWS Gebühren zugreifen.

Um auf Ihre Rechnungsinformationen zuzugreifen

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Wählen Sie auf der Navigationsleiste den Namen Ihres Kontos aus.
3. Wählen Sie Billing and Cost Management.
4. Verwenden Sie das AWS Fakturierung und Kostenmanagement Dashboard, um eine Zusammenfassung und Aufschlüsselung Ihrer monatlichen Ausgaben zu finden.

Melden Sie sich bei mehreren Konten an

Sie können sich in einem einzigen Webbrowser im mit bis zu fünf verschiedenen Identitäten gleichzeitig anmelden. AWS-Managementkonsole Dabei kann es sich um eine beliebige Kombination von Root-, IAM- oder Verbundrollen in verschiedenen Konten oder in demselben Konto handeln. Jede Identität, mit der Sie sich anmelden, öffnet ihre eigene Instanz von auf AWS-Managementkonsole einer neuen Registerkarte.

Wenn Sie die Unterstützung mehrerer Sitzungen aktivieren, enthält die Konsolen-URL eine Subdomain (z. B.`https://000000000000-aaaaaaaa.us-east-1.console.aws.amazon.com/console/home?region=us-east-1`). Achten Sie darauf, Ihre Lesezeichen und Konsolenlinks zu aktualisieren.

> **Note**
>
> Sie müssen sich für die Unterstützung mehrerer Sitzungen anmelden, indem Sie im Kontomenü unter „Mehrere Sitzungen aktivieren“ wählen oder indem Sie „Mehrfachsitzung aktivieren am/“ auswählen. AWS-Managementkonsole https://console.aws.amazon.com Sie können sich jederzeit von der Nutzung mehrerer Sitzungen abmelden, indem Sie „Mehrfachsitzung deaktivieren“ wählen oder indem Sie Ihre Browser-Cookies https://console.aws.amazon.com löschen. Das Opt-In ist browserspezifisch.

Um sich mit mehreren Identitäten anzumelden

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Wählen Sie auf der Navigationsleiste den Namen Ihres Kontos aus.
3. Wählen Sie Sitzung hinzufügen und dann Anmelden aus. Es öffnet sich ein neuer Tab, auf dem Sie sich anmelden können.

> **Note**
>
> Weitere Informationen zur Anmeldung als Root- oder IAM-Benutzer finden Sie im AWS Anmelde-Benutzerhandbuch unter Anmelden am. AWS-Managementkonsole

4. Geben Sie Ihre -Anmeldeinformationen ein.
5. Klicken Sie auf Sign in. Das wird auf dieser Registerkarte als die von Ihnen gewählte AWS Identität AWS-Managementkonsole geladen.
6. (Optional) Um sich zu weiteren Rollen zusammenzuschließen

   a. Melden Sie sich im AWS IAM Identity Center Zugriffsportal oder in Ihrem Single-Sign-On-Portal (SSO) für die zusätzliche Rolle an.

   b. AWS-Managementkonsole Wählen Sie im Menü Ihren Kontonamen aus.

   c. Sehen Sie sich die zusätzlichen Sitzungen an, die Sie auswählen können.

AWS Empfohlene Aktionen in der AWS-Managementkonsole

AWS Empfohlene Aktionen helfen Ihnen dabei, effizienter zu arbeiten, AWS-Managementkonsole indem sie kontextbezogene Vorschläge für die Erledigung von Aufgaben und die Implementierung bewährter Verfahren bereitstellen. Wenn relevante Empfehlungen verfügbar sind, wird eine dynamische Schaltfläche angezeigt, mit der Sie auf der Grundlage dieser Vorschläge schnell Maßnahmen ergreifen können.

> **Note**
>
> AWS Recommended Actions analysiert den Ressourcenstatus, um Vorschläge zu unterbreiten, verarbeitet jedoch keine Benutzerdaten.

Themen

- Merkmale der AWS empfohlenen Aktionen
- Verwenden von empfohlenen Maßnahmen
- API-Aufrufe AWS für empfohlene Aktionen protokollieren mit AWS CloudTrail

Merkmale der AWS empfohlenen Aktionen

- Handlungsempfehlungen — Erhalten Sie relevante Vorschläge auf der Grundlage des Ressourcenstatus, der bewährten Verfahren und der gängigen Nutzungsmuster
- Aktionen mit einem Klick — Führen Sie empfohlene Maßnahmen direkt aus Erfolgsmeldungen oder Ressourcenansichten aus
- Integriertes Bedienfeld auf der rechten Seite — Greifen Sie auf ein integriertes Seitenfenster zu, um Vorschläge umzusetzen, ohne Ihren Arbeitsablauf zu unterbrechen
- Multi-Service-Support — Holen Sie sich Empfehlungen für mehrere Dienste AWS

Verwenden von empfohlenen Maßnahmen

Um empfohlene Aktionen zu verwenden

1. Loggen Sie sich ein bei AWS-Managementkonsole
2. Suchen Sie nach der Schaltfläche # Empfohlene Aktionen.

> **Note**
>
> Die Schaltfläche für empfohlene Aktionen kann an einer beliebigen Stelle im angezeigt werden AWS-Managementkonsole und ist nur verfügbar, wenn empfohlene Aktionen verfügbar sind.

3. Wählen Sie die Schaltfläche, um die verfügbaren Aktionen anzuzeigen.
4. Lassen Sie Empfehlungen direkt oder über das Seitenpanel laufen.

API-Aufrufe AWS für empfohlene Aktionen protokollieren mit AWS CloudTrail

AWS Recommended Actions ist in einen Dienst integriert, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem ausgeführten Aktionen bereitstellt AWS-Service. AWS CloudTrail CloudTrail erfasst alle API-Aufrufe für AWS empfohlene Aktionen als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe der API-Operationen für AWS empfohlene Aktionen AWS-Managementkonsole und Codeaufrufen. Anhand der von gesammelten Informationen können Sie

ermitteln CloudTrail, welche Anfrage an AWS Recommended Actions gestellt wurde, von welcher IP-Adresse aus die Anfrage gestellt wurde, wann sie gestellt wurde, und weitere Details.

CloudTrail ist in Ihrem aktiv AWS-Konto , wenn Sie das Konto erstellen, und Sie haben automatisch Zugriff auf den CloudTrail Eventverlauf. Der CloudTrail Ereignisverlauf bietet eine einsehbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der aufgezeichneten Verwaltungsereignisse der letzten 90 Tage in einem. AWS-Region Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf. Für die Anzeige des Eventverlaufs CloudTrail fallen keine Gebühren an.

Für eine fortlaufende Aufzeichnung der Ereignisse in AWS-Konto den letzten 90 Tagen erstellen Sie einen Trail- oder CloudTrailLake-Event-Datenspeicher.

AWS Verwaltungsereignisse mit empfohlenen Maßnahmen in CloudTrail

Verwaltungsereignisse enthalten Informationen zu Verwaltungsvorgängen, die an Ressourcen in Ihrem ausgeführt werden AWS-Konto. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. CloudTrail Protokolliert standardmäßig Verwaltungsereignisse.

AWS Mit den empfohlenen Aktionen werden alle Vorgänge auf der Kontrollebene mit AWS empfohlenen Aktionen als Verwaltungsereignisse protokolliert.

AWS Beispiele für Ereignisse mit empfohlenen Aktionen

Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über den angeforderten API-Vorgang, Datum und Uhrzeit des Vorgangs, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass Ereignisse nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt ein CloudTrail Ereignis, das den Vorgang demonstriert.


```
{
  "awsRegion": "us-east-2",
  "eventCategory": "Management",
  "eventID": "3510a29e-8070-4cbc-b6a0-9e11f18e26ec",
  "eventName": "ListRecommendedActions",
  "eventSource": "action-recommendations.amazonaws.com",
  "eventTime": "2025-09-03T03:52:02Z",
  "eventType": "AwsApiCall",
  "eventVersion": "1.09",
  "managementEvent": true,
```

```
  "readOnly": true,
  "recipientAccountId": "123456789098",
  "requestID": "ec431c91-0315-413d-bdb6-d282fd4f6d83",
  "requestParameters": {
    "context": "*",
    "uxChannel": "EXAMPLE"
  },
  "responseElements": null,
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "EXAMPLE",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROARZDBH75ZCUYWFSTUS:EXAMPLE",
    "arn": "arn:aws:sts::123456789098:assumed-role/EXAMPLE",
    "accountId": "12345678909",
    "accessKeyId": "ASIARZDBEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AROARZDBHEXAMPLE",
          "arn": "arn:aws:iam::12345678909:role/EXAMPLE",
          "accountId": "12345678909",
          "userName": "EXAMPLE"
        },
        "attributes": {
          "creationDate": "2025-09-03T03:52:00Z",
          "mfaAuthenticated": "false"
        }
      },
    "invokedBy": "action-recommendations.amazonaws.com"
  }
}
```


Informationen zu CloudTrail Datensatzinhalten finden Sie im AWS CloudTrail Benutzerhandbuch unter CloudTrailDatensatzinhalt.

Verwenden AWS Console Home in der AWS-Managementkonsole

In diesem Thema wird beschrieben AWS Console Home, wie Sie Ihre Konsolen-Startseite verwenden und anpassen können. Die Konsolen-Startseite ist die Startseite von AWS-Managementkonsole. Wenn Sie sich zum ersten Mal bei der Konsole anmelden, landen Sie auf der Startseite der Konsole. Sie können Ihre Konsolen-Startseite mithilfe von Widgets und Anwendungen anpassen. Mit Widgets können Sie benutzerdefinierte Komponenten hinzufügen, die Informationen über Ihre AWS Dienste und Ressourcen verfolgen. Mit Anwendungen können Sie Ihre AWS Ressourcen und Metadaten gruppieren. Sie können Anwendungen mit MyApplications verwalten. Sie können auch die Konsolen-Startseite verwenden, um eine Liste aller AWS Dienste anzuzeigen und mit Amazon Q zu chatten.

Themen

Alle AWS Dienste anzeigen in AWS Console Home

Sie können von Console Home aus eine Liste aller AWS Dienste anzeigen und auf deren Konsolen zugreifen.

So greifen Sie auf eine vollständige Liste der AWS Dienste zu

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Erweitern Sie das Home-Menü der Konsole, indem Sie das Hamburger-Symbol (☰) auswählen.
3. Wählen Sie „Alle Dienste“.
4. Wählen Sie einen AWS Dienst aus, um zu seiner Konsole zu navigieren.

Arbeiten mit Widgets in AWS Console Home

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

Widgets verwalten

Sie können Widgets verwalten, indem Sie sie hinzufügen, entfernen, neu anordnen und ihre Größe ändern. Standard-Widgets können entfernt und wieder hinzugefügt werden. Sie können auch die Startseite Ihrer Konsole auf das Standardlayout zurücksetzen und neue Widgets anfordern.

So fügen Sie ein Widget hinzu:

1. Wählen Sie oben oder unten rechts auf dem Dashboard auf der Konsolenstartseite die Schaltfläche Widgets hinzufügen aus.
2. Wählen Sie oben links in der Titelleiste des Widgets den Ziehanzeiger aus, der durch sechs vertikale Punkte () dargestellt wird, und ziehen Sie ihn dann auf Ihr Console-Home-Dashboard.

So entfernen Sie ein Widget

1. Wählen Sie oben rechts in der Titelleiste des Widgets die Ellipse aus, die durch drei vertikale Punkte () dargestellt wird.
2. Wählen Sie Remove widget (Widget entfernen) aus.

So ordnen Sie Ihre Widgets neu an

- Wählen Sie oben links in der Titelleiste des Widgets die Ziehanzeige aus, die durch sechs vertikale Punkte () dargestellt wird, und ziehen Sie das Widget dann an eine neue Position auf Ihrem Console-Home-Dashboard.

So ändern Sie die Größe eines Widgets

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

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

So setzen Sie die Seite auf das Standardlayout zurück:

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

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

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

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

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

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

Worin befindet sich MyApplications? AWS Console Home

myApplications ist eine Erweiterung von Console Home, mit der Sie die Kosten, den Zustand, den Sicherheitsstatus und die Leistung Ihrer Anwendungen in AWS verwalten und überwachen können. Mit Anwendungen können Sie Ressourcen und Metadaten gruppieren. Sie können auf alle Anwendungen in Ihrem Konto, wichtige Kennzahlen für alle Anwendungen und einen Überblick über

Kosten-, Sicherheits- und Betriebsmetriken sowie Erkenntnisse aus mehreren Servicekonsolen von einer Ansicht aus zugreifen AWS-Managementkonsole. myApplications umfasst Folgendes:

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

Themen

Features von myApplications

- Anwendungen erstellen – erstellen Sie neue Anwendungen und organisieren Sie deren Ressourcen. Ihre Anwendungen werden automatisch in MyApplications angezeigt, sodass Sie in der AWS-Managementkonsole, APIs, CLI und SDKs Maßnahmen ergreifen können. Infrastructure as Code (IaC) wird generiert, wenn Sie eine Anwendung erstellen, und ist über das myApplication-Dashboard zugänglich. IaC kann in IaC-Tools wie Terraform verwendet werden. AWS CloudFormation
- Auf Ihre Anwendungen zugreifen – Sie können über das myApplications-Widget schnell auf jede Ihrer Anwendungen zugreifen, indem Sie sie auswählen.
- Greifen Sie auf Ihre Ressourcen zu — Sie können Ihre Anwendungsressourcen schnell im Menü Dienste anzeigen, indem Sie die Anwendung auswählen. Wenn Sie eine Ressource auswählen, gelangen Sie direkt zur entsprechenden Servicekonsole. Ihr Platz in der Ressourcentabelle wird gespeichert, sodass Sie jederzeit über das Menü Dienste weitersurfen können.

- Anwendungsmetriken vergleichen – verwenden Sie myApplications, um wichtige Metriken für Anwendungen wie die Kosten für Anwendungsressourcen und die Anzahl kritischer Sicherheitsergebnisse für mehrere Anwendungen zu vergleichen.
- Anwendungen überwachen und verwalten — Beurteilen Sie den Zustand und die Leistung von Anwendungen anhand von Alarmen, Kanarien und Service-Level-Zielvorgaben Amazon CloudWatch AWS Security Hub CSPM, Ergebnissen und Kostentrends von AWS Cost Explorer Service. Unter finden Sie auch Zusammenfassungen und Optimierungen von Berechnungsmetriken sowie die Verwaltung der Einhaltung von Ressourcenbestimmungen und des Konfigurationsstatus. AWS Systems Manager

Zugehörige Services

myApplications verwendet die folgenden Services:

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

Zugreifen auf myApplications

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

Preisgestaltung

MyApplications on AWS wird ohne zusätzliche Kosten angeboten. Es fallen keine Einrichtungsgebühren oder Vorableistungen an. Die Nutzungsgebühren für die zugrunde liegenden

Ressourcen und Services, die im myApplication-Dashboard zusammengefasst sind, fallen weiterhin zu den für diese Ressourcen veröffentlichten Tarifen an.

Unterstützte Regionen für MyApplications

MyApplications ist in den folgenden Sprachen verfügbar: AWS-Regionen

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

Opt-In-Regionen

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

- Afrika (Kapstadt)
- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Hyderabad)

- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Melbourne)
- Europa (Milan)
- Europa (Spain)
- Europa (Zürich)
- Middle East (Bahrain)
- Naher Osten (VAE)
- Israel (Tel Aviv)

Anwendungen in MyApplications

Mit Anwendungen können Sie Ihre Ressourcen und Metadaten gruppieren. Sie können Ihre Anwendungen verwalten, indem Sie sie erstellen, integrieren, anzeigen, bearbeiten oder löschen. Sie können auch Codefragmente erstellen, um einer Anwendung automatisch neue Ressourcen hinzuzufügen.

> **Note**
>
> Sie können Anwendungen auch zu Ihren Favoriten hinzufügen, damit Sie leichter darauf zugreifen können. Weitere Informationen finden Sie unter ???.

Themen

Anwendungen in MyApplications erstellen

Sie können eine neue oder vor dem 8. November 2023 the section called “Onboarding von Anwendungen” erstellte Anwendung erstellen, um mit MyApplications zu beginnen. Wenn Sie eine

neue Anwendung erstellen, können Sie Ressourcen hinzufügen, indem Sie nach ihnen suchen und sie auswählen oder indem Sie vorhandene Tags verwenden.

So erstellen Sie eine neue Anwendung

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Erweitern Sie die linke Seitenleiste und wählen Sie Meine Anwendungen.
3. Wählen Sie Create application aus.
4. Geben Sie einen Anwendungsnamen ein.
5. (Optional) Geben Sie eine Anwendungsbeschreibung ein.
6. (Optional) Fügen Sie Tags hinzu. Tags sind Schlüssel-Wert-Paare, die auf Ressourcen angewendet werden, um Metadaten zu diesen Ressourcen zu enthalten.

   > **Note**
   >
   > Das AWS Anwendungs-Tag wird automatisch auf neu erstellte Anwendungen angewendet. Weitere Informationen finden Sie im AWS Service Catalog AppRegistry Administratorhandbuch unter Das AWS Anwendungs-Tag.

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

   Search and select resources

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

   Um Ressourcen mithilfe der Suche hinzuzufügen

   1. Wählen Sie Suchen und wählen Sie Ressourcen aus.

2. Wählen Sie Ressourcen auswählen aus.
3. (Optional) Wählen Sie eine Ansicht aus.
4. Suchen Sie nach Ihren Ressourcen. Sie können nach Schlüsselwörtern, Namen oder Typ suchen oder einen Ressourcentyp auswählen.

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

5. Aktivieren Sie das Kontrollkästchen neben den Benutzern, die Sie hinzufügen möchten.
6. Wählen Sie Hinzufügen aus.
7. Wählen Sie Weiter aus.
8. Überprüfen Sie Ihre Auswahl.

Automatically add resources using tags

Wenn Sie eine Anwendung erstellen, können Sie Ressourcen massenweise integrieren, indem Sie ein vorhandenes Tag-Schlüssel-Wert-Paar angeben. Mit dieser Methode wird das `awsApplication` Tag AWS automatisch auf alle Ressourcen angewendet, die mit dem angegebenen Schlüssel-Wert-Paar gekennzeichnet sind, und es wird standardmäßig eine Tag-Synchronisierung für die Ressourcen der Anwendung erstellt. Wenn Tag-Sync aktiviert ist, werden alle Ressourcen, die mit dem angegebenen Tag-Schlüssel-Wert-Paar gekennzeichnet sind, automatisch der Anwendung hinzugefügt. Hinweise zur Behebung von Tag-Synchronisierungsfehlern finden Sie unter. the section called “Fehler bei der Tag-Synchronisierung in MyApplications beheben”

> **Note**
>
> Das Hinzufügen von Ressourcen zu einer Anwendung mithilfe von Tags erfordert Berechtigungen zum Erstellen einer AppRegistry Anwendung, zum Gruppieren und Aufheben der Gruppierung von Ressourcen sowie zum Markieren und Aufheben von Tags für Ressourcen. Sie können entweder die

ResourceGroupsTaggingAPITagUntagSupportedResources AWS verwaltete Richtlinie für Resource Groups hinzufügen oder Ihre eigene benutzerdefinierte Richtlinie erstellen und verwalten. Die folgenden Berechtigungen müssen der Richtlinienerklärung eines Benutzers in IAM hinzugefügt werden:

- `servicecatalog:CreateApplication`
- `resource-groups:GroupResources`
- `resource-groups:UngroupResources`
- `tag:TagResources`
- `tag:UntagResources`

Um Ressourcen mithilfe vorhandener Tags hinzuzufügen

1. Wählen Sie Ressourcen mithilfe von Tags automatisch hinzufügen aus.
2. Wählen Sie einen vorhandenen Tag-Schlüssel und -Wert aus:
   a. Wählen Sie die Rolle aus, die zum Markieren von Ressourcen verwendet wird. Weitere Informationen finden Sie unter Erforderliche Tag-Sync-Berechtigungen im AWS Service AppRegistry Catalog-Administratorhandbuch.
   b. Wählen Sie einen Tag-Schlüssel aus.
   c. Wählen Sie einen Tag-Wert aus.
   d. (Optional) Wählen Sie „Ressourcen in Vorschau anzeigen“, um eine Vorschau der Ressourcen anzuzeigen, die mit dem Tag-Schlüssel-Wert-Paar gekennzeichnet sind.
   e. Überprüfe und akzeptiere die Option Ich bestätige, dass Gruppen-Lifecycle-Ereignisse aktiviert werden, um eine Benachrichtigung zur Tag-Synchronisierung zu erstellen. Mit GLE können Sie Änderungen AWS an den Ressourcen feststellen, die mit Ihrem Schlüssel-Wert-Paar gekennzeichnet sind.
3. Wählen Sie Weiter aus.
4. Überprüfen Sie Ihre Anwendungsdetails, das ausgewählte Tag-Schlüssel-Wert-Paar und die Vorschau der Ressourcen, die der Anwendung hinzugefügt werden.

> **Note**
>
> Standardmäßig wird beim Erstellen einer Anwendung, die ein vorhandenes Tag-Schlüssel-Wert-Paar verwendet, eine Tag-Synchronisierung durchgeführt. Nach der Einrichtung verwaltet Tag-Sync auch kontinuierlich die Ressourcen der Anwendung und fügt Ressourcen hinzu oder entfernt sie, sobald sie mit dem angegebenen Schlüssel-Wert-Paar gekennzeichnet sind oder nicht. Sie können die Tag-Synchronisierung auf der Seite Ressourcen verwalten der Anwendung verwalten.

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

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

11. Wählen Sie Create application aus.

Integrieren Sie bestehende AppRegistry Anwendungen in MyApplications

Sie können eine bestehende AppRegistry Anwendung, die vor dem 8. November 2023 erstellt wurde, einbinden, um mit MyApplications zu beginnen.

Um eine bestehende AppRegistry Anwendung zu integrieren

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Wählen Sie in der linken Seitenleiste myApplications aus.
3. Verwenden Sie die Suchleiste, um nach Ihrer Anwendung zu suchen.
4. Wählen Sie Ihre Anwendung aus.

5. Wählen Sie Onboard***application name***.
6. Wenn Sie einen CloudFormation Stapel zuordnen möchten, aktivieren Sie das Kontrollkästchen im Warnfeld.
7. Wählen Sie Onboarding für Anwendung ausführen aus.

Anwendungen in MyApplications anzeigen

Sie können Ihre Anwendungen über „Meine Anwendungen“ oder das Menü „Dienste“ aufrufen. Wenn Sie Ihre Anwendungen von MyApplications aus aufrufen, können Sie sie für alle AWS-Regionen oder für bestimmte AWS-Regionen Anwendungen zusammen mit den entsprechenden Informationen in einer Karten- oder Tabellenansicht anzeigen.

> **Note**
>
> Sie können auch Anwendungen, die zu Ihren Favoriten hinzugefügt wurden, über das Favoritenmenü anzeigen. Weitere Informationen finden Sie unter Favoriten im AWS-Managementkonsole.

myApplications

Um Anwendungen in „Meine Anwendungen“ anzusehen

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

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

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

g. Wählen Sie Bestätigen aus.

Services menu

Um Anwendungen über das Menü „Dienste“ anzuzeigen

1. Öffnen Sie die AWS-Managementkonsole.
2. Wählen Sie in der Navigationsleiste „Dienste“ („Dienste“) aus.
3. Wählen Sie Alle Anwendungen aus.
4. Wählen Sie eine Anwendung aus.
5. (Optional) Wählen Sie eine Ansicht aus.
6. (Optional) Wählen Sie einen Filter aus. Sie können Ihre Ressourcen nach Eigenschaften oder nach Tags filtern. Weitere Informationen finden Sie im AWS Resource Explorer Benutzerhandbuch unter Syntaxreferenz für Suchabfragen für Resource Explorer.
7. (Optional) Wählen Sie eine Ressource aus, um sie in der entsprechenden Servicekonsole anzuzeigen.

> **Tip**
>
> Sie können dort weiter nach Ressourcen suchen, wo Sie aufgehört haben, indem Sie Dienste () wählen. Ihre angewendeten Suchfilter bleiben ebenfalls bestehen.

Anwendungen in MyApplications bearbeiten

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

So bearbeiten Sie eine Anwendung

1. Öffnen Sie die AWS-Managementkonsole.

2. Wählen Sie in der linken Seitenleiste der Konsole myApplications aus.
3. Wählen Sie die Anwendung aus, die Sie bearbeiten möchten.
4. Wählen Sie im MyApplication-Dashboard Aktionen und dann Anwendung bearbeiten aus.
5. Nehmen Sie unter Anwendung bearbeiten die gewünschten Änderungen an der Beschreibung, den Tags und den Attributgruppen Ihrer Anwendung vor.

> **Note**
>
> Weitere Informationen zur Verwaltung von Tags und Attributgruppen finden Sie unter Tags verwalten und Attributgruppen bearbeiten im AWS Service Catalog AppRegistry Administratorhandbuch.

6. Wählen Sie Aktualisieren aus.

Löschen von Anwendungen in MyApplications

Sie können Anwendungen löschen, wenn sie nicht mehr benötigt werden. Stellen Sie vor dem Löschen einer Anwendung sicher, dass Sie alle zugehörigen Ressourcenfreigaben und Attributgruppen entfernen, die nicht von einem AWS Dienst erstellt wurden.

> **Note**
>
> Das Löschen einer Anwendung hat keine Auswirkungen auf Ihre Ressourcen. Ressourcen, die mit dem AWS Anwendungs-Tag gekennzeichnet sind, bleiben markiert.

So löschen Sie eine -Anwendung

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

Codefragmente in MyApplications erstellen

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

So erstellen Sie einen Codeausschnitt für Ihre Anwendung

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

Ressourcen in „Meine Anwendungen“

In ist eine Ressource eine Entität AWS, mit der Sie arbeiten können. Beispiele hierfür sind eine Amazon EC2 EC2-Instance, ein AWS CloudFormation Stack oder ein Amazon S3 S3-Bucket. Sie können Ihre Ressourcen in MyApplications verwalten, indem Sie sie zu Anwendungen hinzufügen und daraus entfernen.

Themen

- Hinzufügen von Ressourcen in MyApplications
- Ressourcen aus MyApplications entfernen
- Ressourcen in MyApplications anzeigen

Hinzufügen von Ressourcen in MyApplications

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

Anwendungen hinzufügen, indem Sie nach ihnen suchen und sie auswählen oder indem Sie vorhandene Tags verwenden und eine Tag-Synchronisierung durchführen.

Search and select resources

Um Ressourcen zu suchen und auszuwählen

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

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

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

Automatically add resources using tags

Wenn Sie eine Anwendung erstellen, können Sie Ressourcen massenweise integrieren, indem Sie ein vorhandenes Tag-Schlüssel-Wert-Paar angeben. Mit dieser Methode wird das `awsApplication` Tag AWS automatisch auf alle Ressourcen angewendet und standardmäßig eine Tag-Synchronisierung für die Ressourcen der Anwendung erstellt. Wenn Tag-Sync aktiviert ist, werden alle Ressourcen, die mit dem angegebenen Tag-Schlüssel-Wert-Paar gekennzeichnet sind, automatisch zur Anwendung hinzugefügt.

Um Ressourcen mithilfe vorhandener Tags hinzuzufügen

1. Öffnen Sie die AWS-Managementkonsole.

2. Wählen Sie in der linken Seitenleiste der Konsole myApplications aus.
3. Wählen Sie Ressourcen verwalten aus.
4. Wählen Sie „Tag-Synchronisierung erstellen“.
5. Wählen Sie einen vorhandenen Tag-Schlüssel und -Wert aus:
    a. Wählen Sie die Rolle aus, die zum Markieren von Ressourcen verwendet wird. Weitere Informationen finden Sie unter Erforderliche Berechtigungen für die Tag-Sync-Aufgabe im AWS Service AppRegistry Catalog-Administratorhandbuch.
    b. Wählen Sie einen Tag-Schlüssel aus.
    c. Wählen Sie einen Tag-Wert aus.
    d. Lesen und akzeptieren Sie die Option Ich bestätige, dass Group Lifecycle Events aktiviert werden, um eine Benachrichtigung zur Tag-Synchronisierung zu erstellen. Mit GLE können Sie Änderungen AWS an den Ressourcen feststellen, die mit Ihrem Schlüssel-Wert-Paar gekennzeichnet sind.
6. Wählen Sie Tag-Synchronisierung erstellen.

Fehler bei der Tag-Synchronisierung in MyApplications beheben

In diesem Abschnitt werden häufig auftretende Fehler bei der Tag-Synchronisierung und deren Behebung beschrieben. Nachdem Sie versucht haben, den Fehler zu beheben, können Sie die fehlgeschlagene Tag-Synchronisierungsaufgabe erneut versuchen.

- Unzureichende Berechtigungen – Sie verfügen nicht über die erforderlichen Mindestberechtigungen, um die Tag-Synchronisierung zu starten, zu aktualisieren oder abzubrechen. Weitere Informationen finden Sie unter Erforderliche Berechtigungen für Tag-Sync. Nachdem Sie sichergestellt haben, dass die Rolle, die Sie für die Tag-Synchronisierung angegeben haben, über die erforderlichen Mindestberechtigungen verfügt, wiederholen Sie die fehlgeschlagene Tag-Synchronisierungsaufgabe.
- Bereits vorhanden – Für diese Anwendung ist bereits eine Aufgabe mit diesem Schlüssel-Wert-Paar für das Tag vorhanden. Eine Anwendung kann mehr als eine Tag-Synchronisierung unterstützen. Jede Tag-Synchronisierung muss jedoch ein anderes Schlüssel-Wert-Paar für das Tag verwenden. Nachdem Sie ein anderes Schlüssel-Wert-Paar für das Tag angegeben haben, versuchen Sie die fehlgeschlagene Tag-Synchronisierungsaufgabe erneut.
- Höchstgrenze erreicht – Sie haben das Maximum von 100 Tag-Synchronisierungsaufgaben pro Konto für alle Anwendungen erreicht.

Ressourcen aus MyApplications entfernen

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

So entfernen Sie Ressourcen

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

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

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

Ressourcen in MyApplications anzeigen

Sie können Ihre Anwendungsressourcen in MyApplications und im Menü Services einsehen.

myApplications

Um Ihre Ressourcen in MyApplications einzusehen

1. Öffnen Sie die AWS-Managementkonsole.
2. Erweitern Sie die linke Seitenleiste und wählen Sie Meine Anwendungen.
3. Wählen Sie eine Anwendung aus.
4. Sehen Sie sich im Ressourcen-Widget Ihre Ressourcen an.

Services menu

Um Anwendungen über das Menü „Dienste“ anzuzeigen

1. Öffnen Sie die AWS-Managementkonsole.
2. Wählen Sie in der Navigationsleiste „Dienste“ („Dienste“) aus.
3. Wählen Sie Alle Anwendungen aus.
4. Wählen Sie eine Anwendung aus.
5. (Optional) Wählen Sie eine Ansicht aus.
6. (Optional) Wählen Sie einen Filter aus. Sie können Ihre Ressourcen nach Eigenschaften oder nach Tags filtern. Weitere Informationen finden Sie im AWS Resource Explorer Benutzerhandbuch unter Syntaxreferenz für Suchabfragen für Resource Explorer.
7. (Optional) Wählen Sie eine Ressource aus, um sie in der entsprechenden Servicekonsole anzuzeigen.

> **Tip**
>
> Sie können dort weiter nach Ressourcen suchen, wo Sie aufgehört haben, indem Sie Dienste () wählen. Ihre angewendeten Suchfilter bleiben ebenfalls bestehen.

Mein Applications-Dashboard in AWS Console Home

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

Themen

- Widget zur Einrichtung des Anwendungs-Dashboards
- Widget mit der Zusammenfassung der Anwendung
- Computing-Widget
- Kosten- und Nutzungs-Widget
- AWS Sicherheits-Widget

- AWS Widget „Resilienz“
- Widget „Ressourcen“
- DevOps Widget
- Widget für Überwachung und Betrieb
- Tags-Widget

Widget zur Einrichtung des Anwendungs-Dashboards

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

Widget mit der Zusammenfassung der Anwendung

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

Computing-Widget

Dieses Widget zeigt Informationen und Metriken für Computing-Ressourcen an, die Sie Ihrer Anwendung hinzufügen. Dazu gehören die Gesamtzahl der Alarme und die Gesamtzahl der Computing-Ressourcentypen. Das Widget zeigt auch Trenddiagramme zur Ressourcenleistungsmetrik Amazon CloudWatch für die CPU-Auslastung von Amazon EC2 EC2-Instances und Lambda-Aufrufe.

Konfigurieren des Computing-Widgets

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

Kosten- und Nutzungs-Widget

Dieses Widget zeigt AWS Kosten- und Nutzungsdaten für Ihre Anwendungsressourcen. Sie können diese Daten verwenden, um die monatlichen Kosten zu vergleichen und die Aufschlüsselung der Kosten nach AWS-Service einzusehen. Dieses Widget fasst nur die Kosten für Ressourcen zusammen, die mit dem AWS Anwendungs-Tag gekennzeichnet sind, ohne Steuern, Gebühren und

andere gemeinsame Kosten, die nicht direkt mit einer Ressource verknüpft sind. Die angezeigten Kosten sind unverschlüsselt und werden mindestens einmal alle 24 Stunden aktualisiert. FOr Weitere Informationen finden Sie unter Analysieren Ihrer Kosten mit AWS Resource Explorer im AWS Cost Management Benutzerhandbuch.

Konfigurieren des Widgets für Kosten- und Nutzung

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

AWS Sicherheits-Widget

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

Konfiguration des AWS Sicherheits-Widgets

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

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

AWS Widget „Resilienz“

Dieses Widget zeigt Resilienzdetails von AWS Resilience Hub für Ihre Anwendungen an. Nach der Initiierung einer Bewertung analysiert AWS Resiliency Hub die Ausfallsicherheit Ihrer Anwendungen, indem die Ressourcen anhand einer vordefinierten Resilienzrichtlinie bewertet werden. Sie

können auf Kennzahlen wie den Resilienzwert, Richtlinienverstöße, Richtlinienabweichungen, Ressourcenabweichungen und den Verlauf Ihrer Resilienzbewertung zugreifen. Ihre Anwendungen werden täglich überprüft, um eine verbesserte Nachverfolgung zu gewährleisten. Sie können diese Funktion jedoch jederzeit deaktivieren. Weitere Informationen finden Sie unter AWS Resilience Hub. Preisinformationen finden Sie unter AWS Resilience Hub Preise.

Konfiguration des AWS Resilienz-Widgets

Um das AWS Resiliency-Widget zu konfigurieren, fügen Sie eine Anwendung hinzu. Weitere Informationen finden Sie unter Was ist AWS Resilience Hub? im AWS Resilience Hub Benutzerhandbuch.

Widget „Ressourcen“

Dieses Widget verwendet den AWS Ressourcen-Explorer, um Ressourcen, die Sie Ihrer Anwendung hinzugefügt haben, in einer Ansicht anzuzeigen. Sie können dieses Widget auch verwenden, um Ihre Ressourcen mithilfe von Ressourcenmetadaten wie Namen, Tags und zu filtern IDs. Weitere Informationen finden Sie unter AWS Resource Explorer.

Konfiguration des Ressourcen-Widgets

Verwenden Sie Resource Explorer, um das Ressourcen-Widget zu konfigurieren. Weitere Informationen finden Sie unter Erste Schritte mit Resource Explorer im AWS Resource Explorer-Benutzerhandbuch.

DevOps Widget

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

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

Konfiguration des DevOps Widgets

Um das DevOps Widget zu konfigurieren, aktivieren Sie es AWS Systems Manager OpsCenter für Ihre Anwendung und Ihr Konto. Weitere Informationen finden Sie unter Erste Schritte mit Systems

Manager Explorer und OpsCenter im AWS Systems Manager Benutzerhandbuch. OpsCenter Durch die Aktivierung können AWS Systems Manager Explorer sie konfiguriert AWS Config werden, Amazon CloudWatch sodass ihre Ereignisse automatisch auf der OpsItems Grundlage häufig verwendeter Regeln und Ereignisse erstellt werden. Weitere Informationen finden Sie OpsCenter im AWS Systems Manager Benutzerhandbuch unter Einrichtung.

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

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

Preisinformationen finden Sie unter AWS Systems Manager Preise.

Widget für Überwachung und Betrieb

Dieses Widget zeigt:

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

Konfigurieren des Widgets für Überwachung und Betrieb

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

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

Tags-Widget

Dieses Widget zeigt alle mit Ihrer Anwendung verknüpften Tags an. Sie können mit diesem Widget Anwendungsmetadaten (Kritikalität, Umgebung, Kostenstelle) verfolgen und verwalten. Weitere

Informationen finden Sie unter Was sind Tags? im AWS Whitepaper Bewährte Methoden zum Kennzeichnen von AWS Ressourcen.

Chatten mit Amazon Q Developer in AWS Console Home

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

Erste Schritte mit Amazon Q

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

Beispielfragen

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

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

AWS-Managementkonsole Privater Zugang

AWS-Managementkonsole Private Access ist eine erweiterte Sicherheitsfunktion zur Steuerung des Zugriffs auf AWS-Managementkonsole. Console Private Access ist nützlich, wenn Sie verhindern möchten, dass sich Benutzer unerwartet AWS-Konten von Ihrem Netzwerk aus anmelden. Mit dieser Funktion können Sie den AWS-Managementkonsole Zugriff auf bestimmte Daten beschränken, von AWS-Konten denen bekannt ist, wann der Datenverkehr aus Ihrem Netzwerk stammt. Der private Zugriff auf die Konsole ist auch nützlich, wenn Sie sicherstellen möchten, dass alle Anrufe von AWS-Managementkonsole an aus Ihrem Netzwerk und von zugelassenen Konten AWS-Services stammen.

Topics

AWS-Regionen Unterstützte Servicekonsolen und Funktionen für Private Access

AWS-Managementkonsole Private Access unterstützt nur eine Teilmenge von Regionen und AWS Diensten. Nicht unterstützte Servicekonsolen werden in der AWS-Managementkonsole inaktiv sein. Darüber hinaus können bestimmte AWS-Managementkonsole Funktionen deaktiviert sein, wenn Sie AWS-Managementkonsole Private Access verwenden, z. B. die Auswahl der Standardregion in den Unified Settings.

Die folgenden Regionen und Servicekonsolen werden unterstützt.

Unterstützte Regionen

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

- USA West (Nordkalifornien)
- USA West (Oregon)
- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Seoul)
- Asien-Pazifik (Osaka)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Malaysia)
- Asien-Pazifik (Thailand)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Europe (Frankfurt)
- Europa (Irland)
- Europa (London)
- Europe (Paris)
- Europa (Stockholm)
- Südamerika (São Paulo)
- Afrika (Kapstadt)
- Asia Pacific (Hongkong)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Melbourne)
- Kanada West (Calgary)
- Mexiko (Zentral)
- Europa (Milan)
- Europa (Spain)
- Europa (Zürich)
- Middle East (Bahrain)
- Naher Osten (VAE)

- Israel (Tel Aviv)

Unterstützte Servicekonsolen

- Amazon API Gateway
- AWS App Mesh
- AWS Application Migration Service
- AWS Artifact
- Amazon Athena
- AWS Audit Manager
- AWS Auto Scaling
- AWS Batch
- AWS Billing Conductor
- AWS Fakturierung und Kostenmanagement
- AWS Budgets
- AWS Certificate Manager
- AWS Cloud Map
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon CodeGuru
- AWS CodePipeline
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Compute Optimizer

- AWS Console Home
- AWS Control Tower
- Amazon DataZone
- AWS Database Migration Service
- AWS DataSync
- AWS DeepRacer
- AWS Direct Connect
- AWS Directory Service
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 Global View
- EC2 Image Builder
- Amazon EC2 Instance Connect
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- AWS Elastic Disaster Recovery
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Elastic Load Balancing
- Amazon ElastiCache
- Amazon EMR
- Amazon EventBridge
- AWS Firewall Manager
- GameLift Amazon-Server
- AWS Glue
- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station

- Amazon GuardDuty
- AWS IAM Identity Center
- AWS Identity and Access Management
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- Amazon Kendra
- AWS Key Management Service
- Amazon Kinesis
- Amazon Managed Service für Apache Flink
- Amazon Data Firehose
- Amazon Kinesis Data Streams
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Managed Grafana
- Amazon Macie
- Amazon Managed Streaming für Apache Kafka
- Amazon Managed Workflows for Apache Airflow (MWAA)
- Strategieempfehlungen von AWS Migration Hub
- Amazon MQ
- Network Access Analyzer
- AWS Network Firewall
- AWS Network Manager
- OpenSearch Amazon-Dienst
- AWS Organizations
- AWS Private Certificate Authority
- Dashboard zur öffentlichen Health
- Amazon Rekognition

- Amazon Relational Database Service
- AWS Resource Access Manager
- AWS -Ressourcengruppen und Tag-Editor
- Amazon Route 53 Resolver
- Amazon Route 53 Resolver DNS-Firewall
- Amazon S3 on Outposts
- Amazon SageMaker
- Amazon SageMaker Runtime
- Synthetische Amazon SageMaker AI-Daten
- AWS Secrets Manager
- AWS Service Catalog
- AWS Security Hub CSPM
- Service Quotas
- AWS Signer
- Amazon Simple Email Service
- Amazon SNS
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon-S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Storage Gateway
- Support
- AWS Systems Manager
- Amazon Timestream
- AWS Transfer Family
- AWS Trusted Advisor
- Vereinheitlichte Einstellungen
- Amazon VPC IP Address Manager
- Amazon Virtual Private Cloud
- Amazon WorkSpaces Thin Client

Überblick über die Sicherheitskontrollen von AWS-Managementkonsole Private Access

Kontoeinschränkungen für das AWS-Managementkonsole von Ihrem Netzwerk aus

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

Konnektivität von Ihrem Netzwerk zum Internet

Für den Zugriff auf Ressourcen, die von verwendet werden AWS-Managementkonsole, wie z. B. statische Inhalte (CSS, Bilder)JavaScript, ist weiterhin eine Internetverbindung von Ihrem Netzwerk aus erforderlich, die alle AWS-Services nicht aktiviert sind AWS PrivateLink. Eine Liste der Top-Level-Domains, die von der verwendet werden AWS-Managementkonsole, finden Sie unterFehlerbehebung.

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

Erforderliche VPC-Endpunkte und DNS-Konfiguration

AWS-Managementkonsole Für Private Access sind die folgenden zwei VPC-Endpunkte pro Region erforderlich. Ersetzen Sie es *`region`* durch Ihre eigenen Regionsinformationen.

1. com.amazonaws. *`region`*.console für AWS-Managementkonsole
2. com.amazonaws. *`region`*. melden Sie sich an für AWS-Anmeldung

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

Topics

DNSKonfiguration für und AWS-Managementkonsole AWS-Anmeldung

Um Ihren Netzwerkverkehr an die jeweiligen VPC-Endpunkte weiterzuleiten, konfigurieren Sie DNS-Datensätze in dem Netzwerk, von dem aus Ihre Benutzer auf die AWS-Managementkonsole zugreifen. Diese DNS-Datensätze leiten den Browserverkehr Ihrer Benutzer zu den von Ihnen erstellten VPC-Endpunkten weiter.

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

- Melden Sie sich an
  - *`region`*.signin.aws.amazon.com zeigt auf den AWS-Anmeldung VPC-Endpunkt in der Anmeldezone, wo sich die gewünschte Region befindet DNS *`region`*
  - signin.aws.amazon.com zeigt auf den AWS Sign-In VPC-Endpunkt in USA Ost (Nord-Virginia) (us-east-1)
- Konsole

- *region*.console.aws.amazon.com zeigt auf den AWS-Managementkonsole VPC-Endpunkt in der Konsolenzone, wo sich die gewünschte Region befindet DNS *region*
- *. *region*.console.aws.amazon.com zeigt auf den AWS-Managementkonsole VPC-Endpunkt in der Konsolenzone, wo sich die gewünschte Region befindet DNS *region*
- *. *region*.console.aws.amazon.com zeigt auf den VPC-Endpunkt in der AWS-Managementkonsole Konsolenzone DNS
- Regionslose CNAME-Datensätze nur für die Region USA Ost (Nord-Virginia). Sie müssen immer die Region US East (Nord-Virginia) einrichten.
  - signin.aws.amazon.com zeigt auf den AWS-Anmeldung VPC-Endpunkt in USA Ost (Nord-Virginia) (us-east-1)
  - *.console.aws.amazon.com zeigt auf den AWS-Managementkonsole VPC-Endpunkt in USA Ost (Nord-Virginia) (us-east-1)

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

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

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

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

Die folgenden `json` Dateien enthalten die vollständige Liste der AWS-Service Endpunkte und Konsolenendpunkte, die pro Region konfiguriert werden müssen. Verwenden Sie das `PrivateIpv4DnsNames`-Feld unter dem `com.amazonaws.`*region*`.console`-Endpunkt für die DNS-Namen.

- https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
- https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
- https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json

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

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

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

- console.aws.amazon.com
- signin.aws.amazon.com
- *. *region*.console.aws.amazon.com
- *region*.console.aws.amazon.com
- *. *region*.console.aws.amazon.com
- signin.aws.amazon.com
- *region*.signin.aws.amazon.com
- Zusätzliche Datensätze in den zuvor aufgelisteten JSON-Dateien

VPC-Endpunkte und DNS Konfiguration für AWS Dienste in der AWS-Managementkonsole

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

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

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

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

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

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

Implementieren von Service-Kontrollrichtlinien und von VPC-Endpunktrichtlinien

Sie können Dienststeuerungsrichtlinien (SCPs) und VPC-Endpunktrichtlinien für AWS-Managementkonsole privaten Zugriff verwenden, um die Anzahl der Konten einzuschränken, die innerhalb Ihrer VPC und der AWS-Managementkonsole damit verbundenen lokalen Netzwerke verwendet werden dürfen.

Topics

- AWS-Managementkonsole Private Access mit AWS Organizations Dienststeuerungsrichtlinien verwenden
- Erlaube die AWS-Managementkonsole Verwendung nur für erwartete Konten und Organisationen (vertrauenswürdige Identitäten)

AWS-Managementkonsole Private Access mit AWS Organizations Dienststeuerungsrichtlinien verwenden

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

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

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

Weitere Informationen zu SCPs finden Sie unter Richtlinien zur Servicesteuerung (SCPs) im AWS Organizations Benutzerhandbuch.

Erlaube die AWS-Managementkonsole Verwendung nur für erwartete Konten und Organisationen (vertrauenswürdige Identitäten)

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

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

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

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

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

JSON

```
{
```

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

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

JSON

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

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

Implementierung identitätsbasierter Richtlinien und anderer Richtlinientypen

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

Unterstützte Kontextschlüssel für AWS globale Bedingungen

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

So funktioniert AWS-Managementkonsole Private Access mit aws: SourceVpc

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

Nachdem sich ein Benutzer bei angemeldet hat AWS-Managementkonsole, stellt er Anfragen AWS-Services über eine Kombination aus direkten Browseranfragen und Anfragen, die von AWS-

Managementkonsole Webservern an Server weitergeleitet werden. AWS Anfragen zu CloudWatch Grafikdaten werden beispielsweise direkt vom Browser aus gestellt. Einige Anfragen an die AWS Servicekonsole, wie Amazon S3, werden dagegen vom Webserver per Proxy an Amazon S3 weitergeleitet.

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

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

> **Note**
>
> Wenn Ihre Benutzer Zugriff auf Servicekonsolen benötigen, die nicht von AWS-Managementkonsole Private Access unterstützt werden, müssen Sie eine Liste Ihrer erwarteten öffentlichen Netzwerkadressen (z. B. Ihren On-Premises-Netzwerkbereich)

hinzufügen, indem Sie den `aws:SourceIP`-Bedingungsschlüssel in den identitätsbasierten Richtlinien der Benutzer verwenden.

Wie sich unterschiedliche Netzwerkpfade widerspiegeln in CloudTrail

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

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

Bei Anfragen, die vom AWS-Managementkonsole Webserver als Proxy weitergeleitet werden, enthalten die CloudTrail Ereignisse keine VPC-bezogenen Details. Erste Anfragen, AWS-Anmeldung die für die Einrichtung der Browsersitzung erforderlich sind, wie z. B. der `AwsConsoleSignIn` Ereignistyp, enthalten jedoch die AWS-Anmeldung VPC-Endpunkt-ID in den Ereignisdetails.

Versuchen Sie es AWS-Managementkonsole mit Private Access

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

AWS-Managementkonsole Private Access ist eine erweiterte Sicherheitsfunktion und erfordert Vorkenntnisse in Bezug auf Netzwerke und Einrichtung VPCs. In diesem Thema wird beschrieben, wie Sie AWS-Managementkonsole Private Access ohne eine umfassende Infrastruktur ausprobieren können.

Themen

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

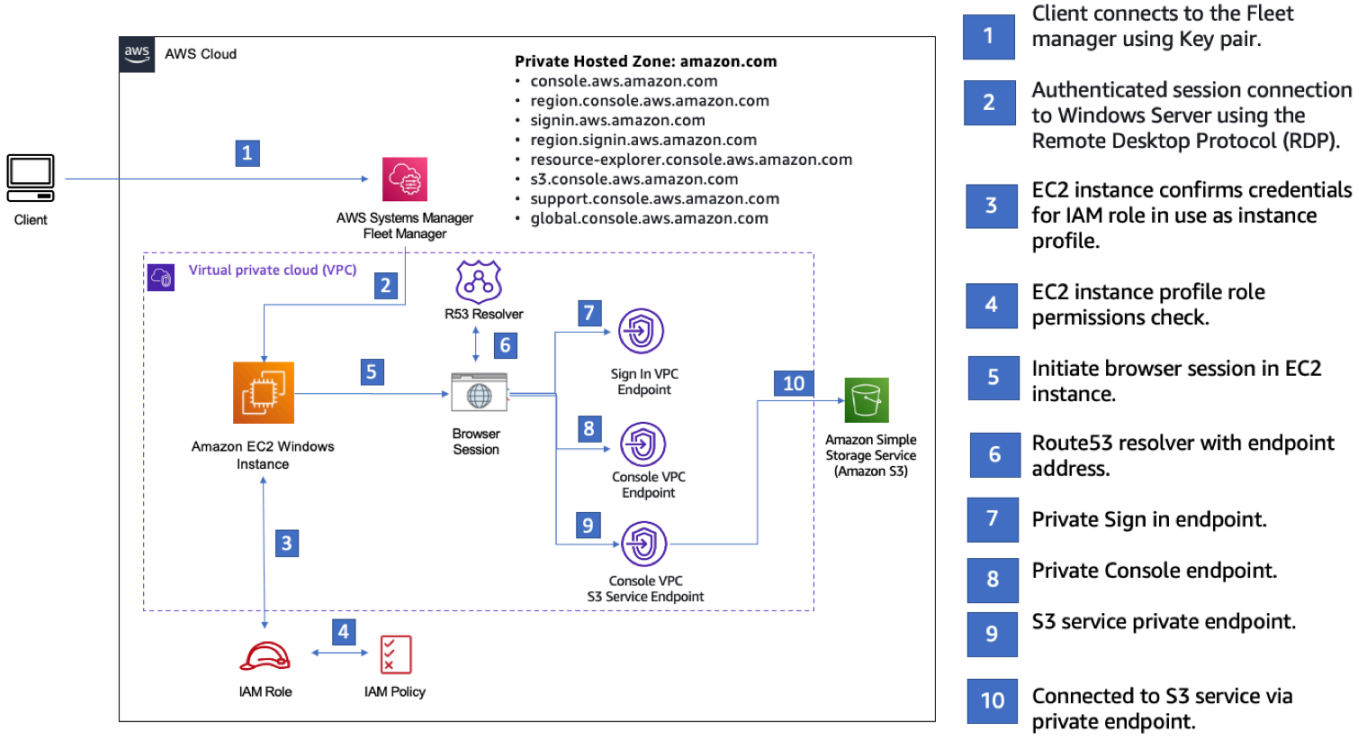
Test-Setup mit Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der Amazon Web Services Cloud. Mit Amazon EC2 können Sie so viele oder so wenige virtuelle Server starten,

wie Sie benötigen, die Sicherheit und das Netzwerk konfigurieren und den Speicher verwalten. Bei dieser Einrichtung verwenden wir Fleet Manager, eine Funktion von AWS Systems Manager, um eine Verbindung zu Ihrer Amazon EC2 Windows Instance mithilfe des Remote Desktop Protocol (RDP) herzustellen.

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

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



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

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

AWS-Managementkonsole Amazon EC2 CloudFormation EC2-Vorlage für private Zugriffsumgebung

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

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

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

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

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

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

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
```

```
    Description: CIDR range for Private Subnet B

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

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

  InstanceTypeParameter:
    Type: String
    Default: 't3.medium'


Resources:

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

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

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

  PublicSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
```

```
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet2CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 1
          - Fn::GetAZs: ""

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

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

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

  PrivateSubnetC:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet3CIDR
```

```
      AvailabilityZone:
        Fn::Select:
          - 2
          - Fn::GetAZs: ""

  InternetGateway:
    Type: AWS::EC2::InternetGateway

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

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

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

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

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

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

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

```
      SubnetId: !Ref PrivateSubnetA

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

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

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

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

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

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

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

```
##########################
# SECURITY GROUPS
##########################

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

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

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

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

  VPCEndpointInterfaceSSM:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
```

```
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssm'
      VpcId: !Ref AppVPC

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

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

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
```

```
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

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

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

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

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

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

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

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

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

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

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

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

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

 SigninHostedZone:
   Type: "AWS::Route53::HostedZone"
   Properties:
     HostedZoneConfig:
```

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

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

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

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

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

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

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

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

So richten Sie ein Netzwerk ein:

1. Melden Sie sich bei dem Verwaltungskonto Ihrer Organisation an, und öffnen Sie die CloudFormation -Konsole.
2. Wählen Sie Stack erstellen aus.
3. Wählen Sie Mit neuen Ressourcen (Standard). Laden Sie die CloudFormation Vorlagendatei hoch, die Sie zuvor erstellt haben, und wählen Sie Weiter.

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

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

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

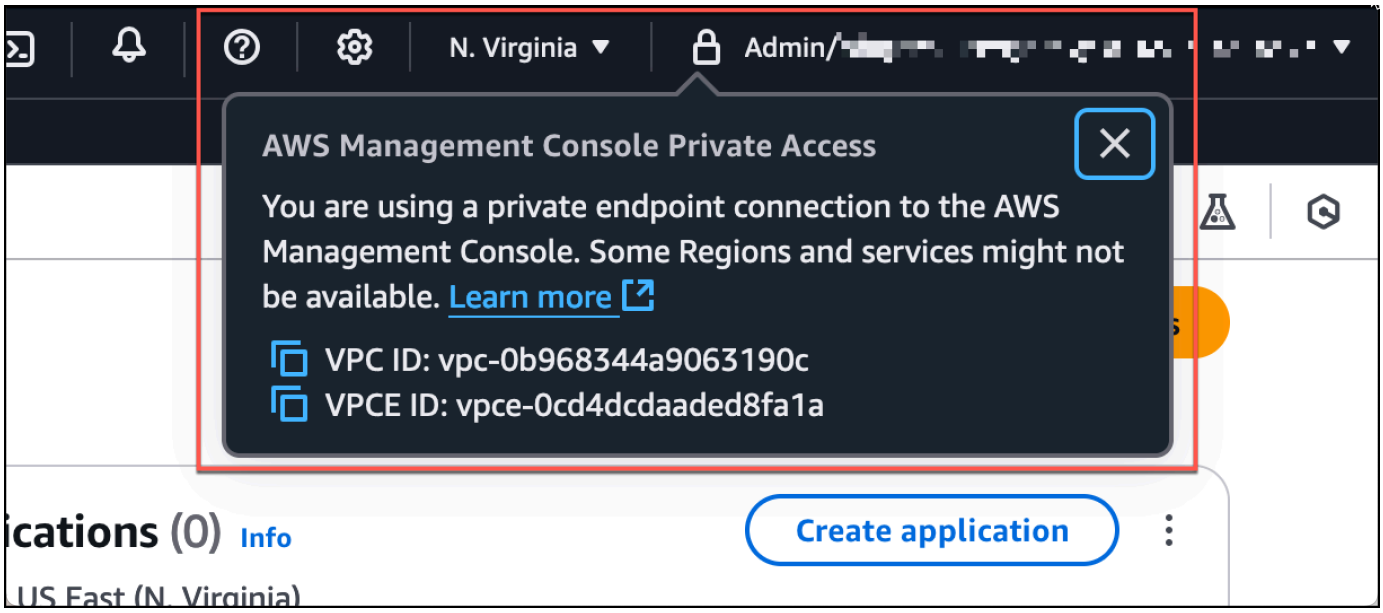
> **Note**
>
> In diesem Beispiel wird Fleet Manager, eine Funktion von AWS Systems Manager Explorer, verwendet, um eine Verbindung zu Ihrem Windows Server herzustellen. Es kann einige Minuten dauern, bis die Verbindung hergestellt werden kann.

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

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

Um die Einrichtung von AWS-Managementkonsole Private Access zu testen

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



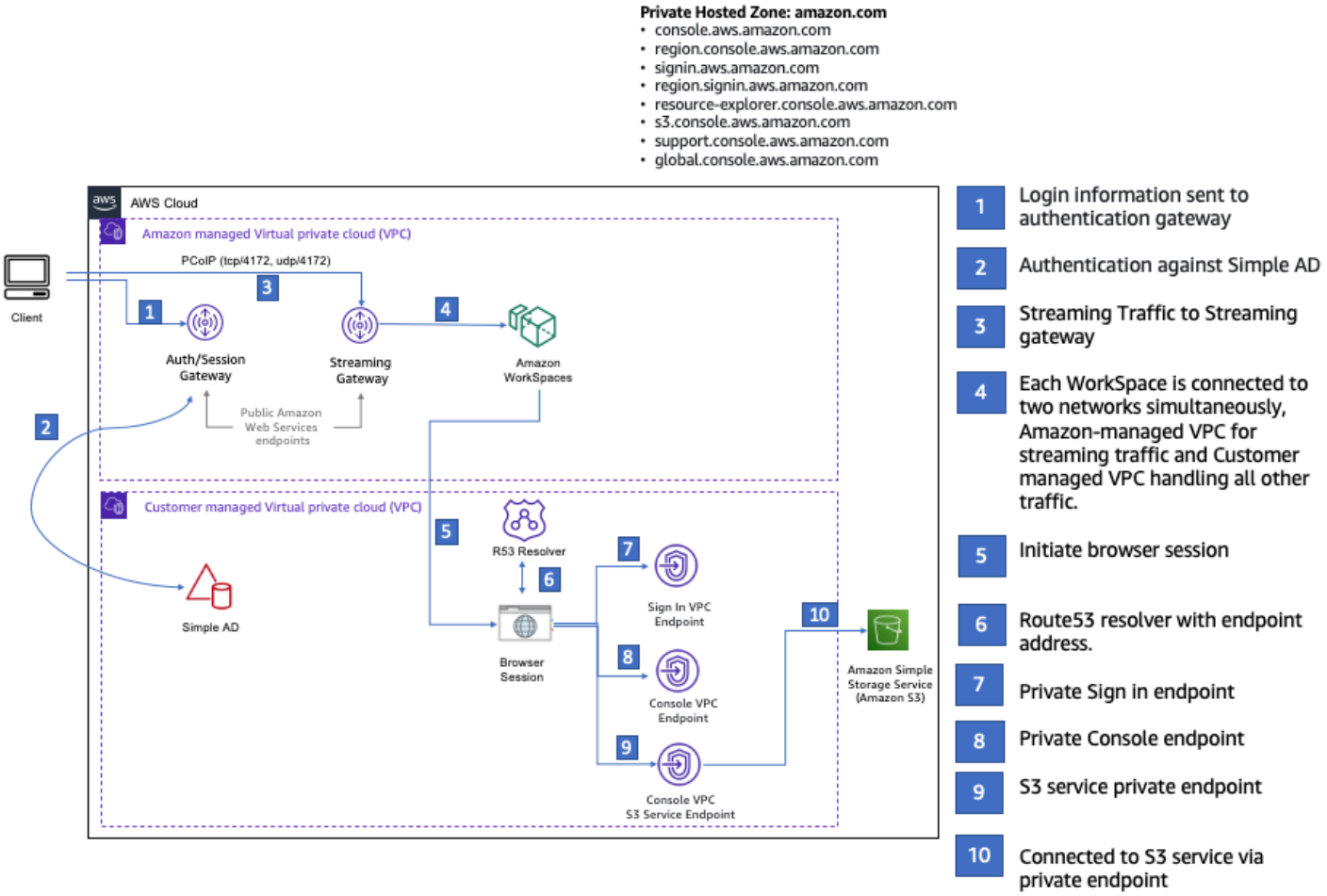
Test-Setup mit Amazon WorkSpaces

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

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

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

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



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

AWS-Managementkonsole CloudFormation Vorlage für eine private Zugriffsumgebung

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

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

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

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

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

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

  DSAdminPasswordResourceName:
    Type: String
    Default: ADAdminSecret
    Description: Password for directory services admin

# Amazon WorkSpaces is available in a subset of the Availability Zones for each
 supported Region.
# https://docs.aws.amazon.com/workspaces/latest/adminguide/azs-workspaces.html
Mappings:
  RegionMap:
```

```
    us-east-1:
      az1: use1-az2
      az2: use1-az4
      az3: use1-az6
    us-west-2:
      az1: usw2-az1
      az2: usw2-az2
      az3: usw2-az3
    ap-south-1:
      az1: aps1-az1
      az2: aps1-az2
      az3: aps1-az3
    ap-northeast-2:
      az1: apne2-az1
      az2: apne2-az3
    ap-southeast-1:
      az1: apse1-az1
      az2: apse1-az2
    ap-southeast-2:
      az1: apse2-az1
      az2: apse2-az3
    ap-northeast-1:
      az1: apne1-az1
      az2: apne1-az4
    ca-central-1:
      az1: cac1-az1
      az2: cac1-az2
    eu-central-1:
      az1: euc1-az2
      az2: euc1-az3
    eu-west-1:
      az1: euw1-az1
      az2: euw1-az2
    eu-west-2:
      az1: euw2-az2
      az2: euw2-az3
    sa-east-1:
      az1: sae1-az1
      az2: sae1-az3

Resources:

  iamLambdaExecutionRole:
    Type: AWS::IAM::Role
```

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

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

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

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

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

  getAZ1:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az1 ]
  getAZ2:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az2 ]

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

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

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

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

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

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

  InternetGateway:
    Type: AWS::EC2::InternetGateway

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

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

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

##########################
# Route Tables
##########################
```

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

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

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

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

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

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

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

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


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

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

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

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

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
```

```
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

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

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

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

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

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

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

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

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

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

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

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

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

 SigninHostedZone:
   Type: "AWS::Route53::HostedZone"
   Properties:
     HostedZoneConfig:
```

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

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

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

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

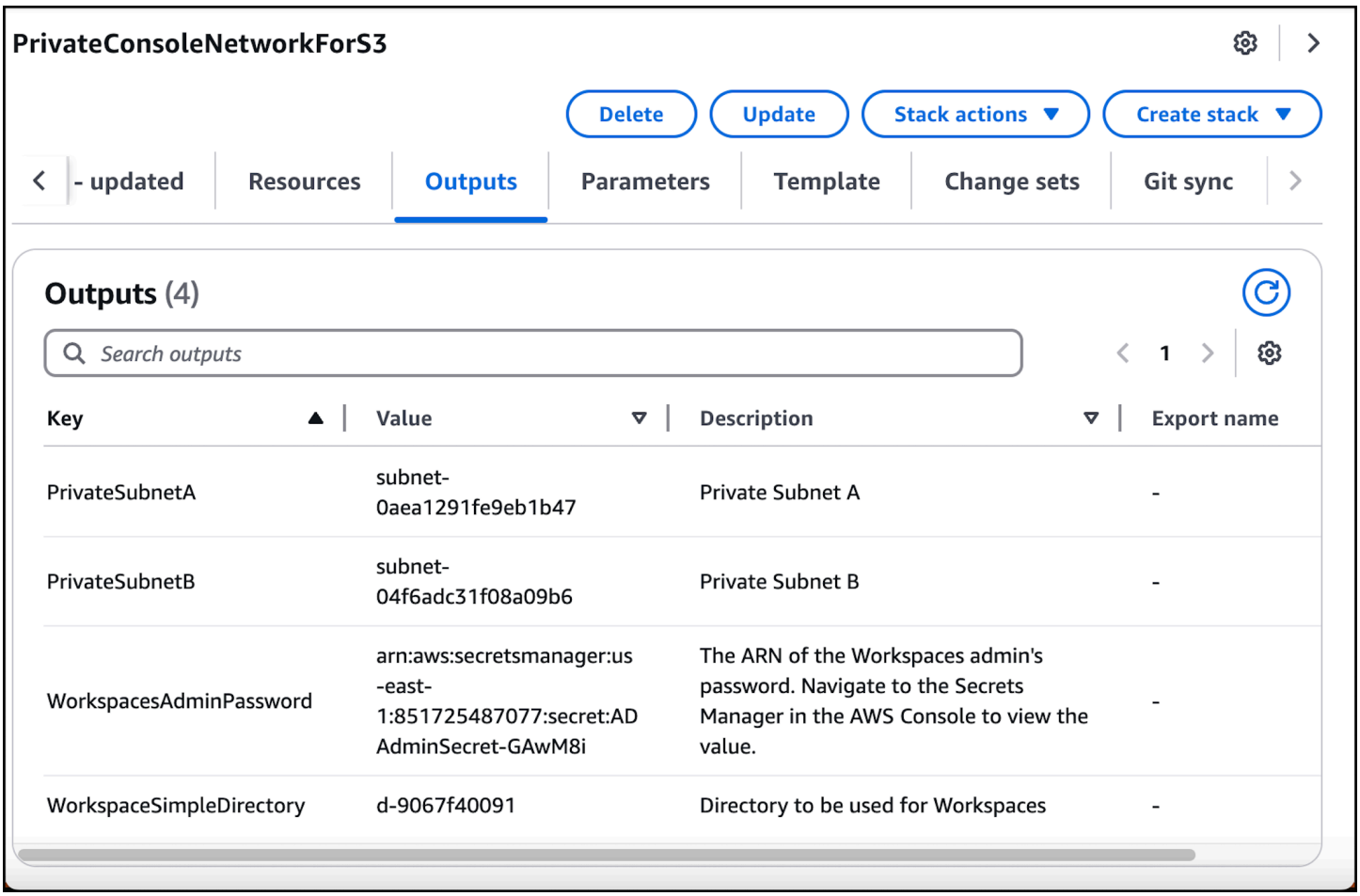
```
  WorkspaceSimpleDirectory:
    Type: AWS::DirectoryService::SimpleAD
    DependsOn: AppVPC
    Properties:
      Name: "corp.awsconsole.com"
      Password: '{{resolve:secretsmanager:ADAdminSecret:SecretString:password}}'
      Size: "Small"
      VpcSettings:
        SubnetIds:
          - Ref: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

        VpcId:
          Ref: AppVPC


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

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

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

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

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

So richten Sie ein Netzwerk ein:

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

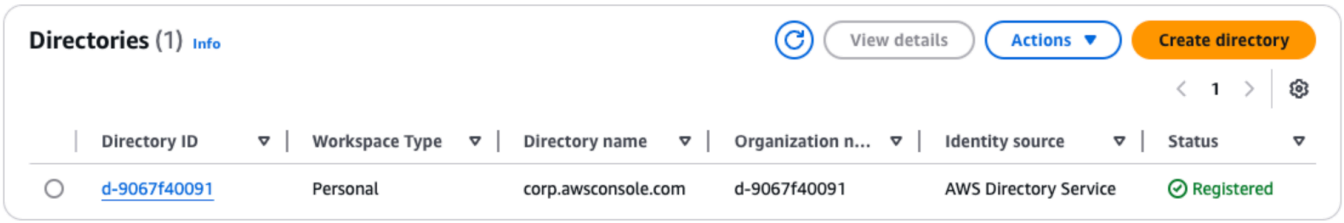
Der folgende Screenshot zeigt die Ansicht der Registerkarte Ausgaben, in der die Werte für die privaten Subnetze und das Workspace Simple Directory angezeigt werden.



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

Um ein zu erstellen WorkSpace

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



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

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

Um auf eine zuzugreifen WorkSpace

1. Öffnen Sie die E-Mail, die Sie in Schritt 14 des vorherigen Verfahrens erhalten haben.
2. Wählen Sie in der E-Mail den eindeutigen Link aus, mit dem Sie Ihr Profil einrichten und den WorkSpaces Client herunterladen können.
3. Richten Sie ihr Passwort ein.
4. Laden Sie den Client Ihrer Wahl herunter.

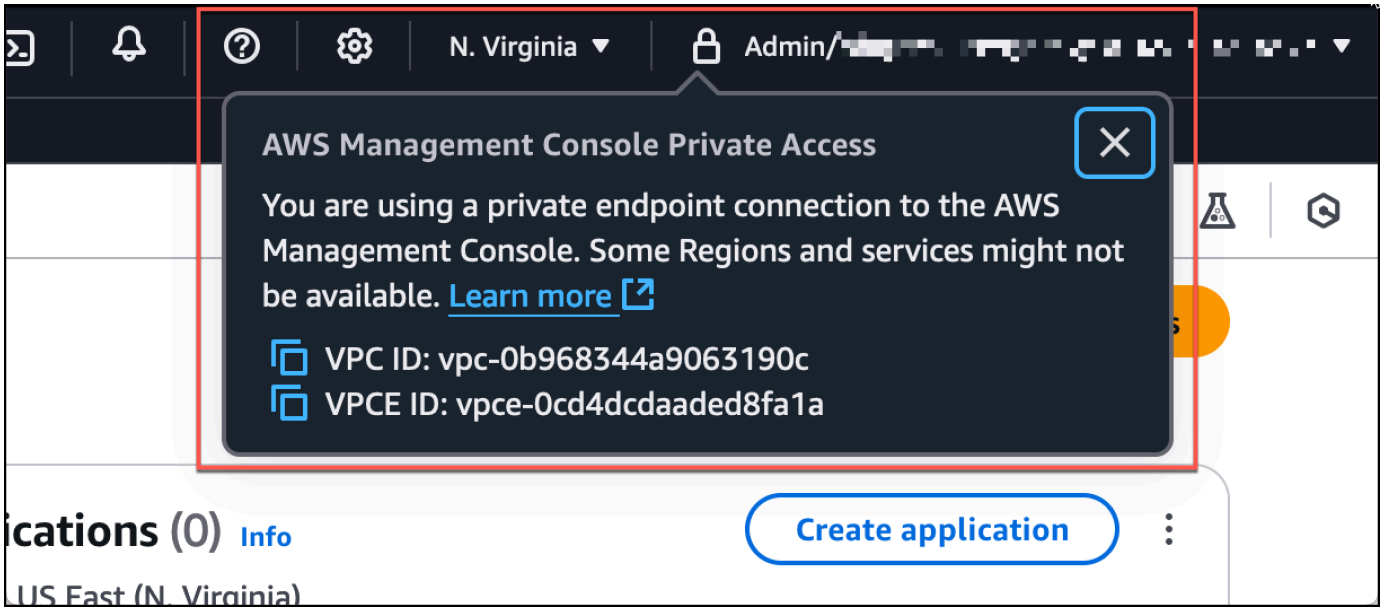
5. Installieren und starten Sie den Client. Geben Sie den Registrierungscode ein, der in Ihrer E-Mail angegeben wurde, und wählen Sie dann Registrieren.
6. Melden Sie sich WorkSpaces mit den Anmeldedaten, die Sie in Schritt 3 erstellt haben, bei Amazon an.

Um die Einrichtung von AWS-Managementkonsole Private Access zu testen

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

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

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



Testen des VPC-Setups mit IAM-Richtlinien

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

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

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "S3:*",
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": "vpc-12345678"
                },
                "Bool": {
                    "aws:ViaAwsService": "false"
                }
            }
        }
    ]
}
```

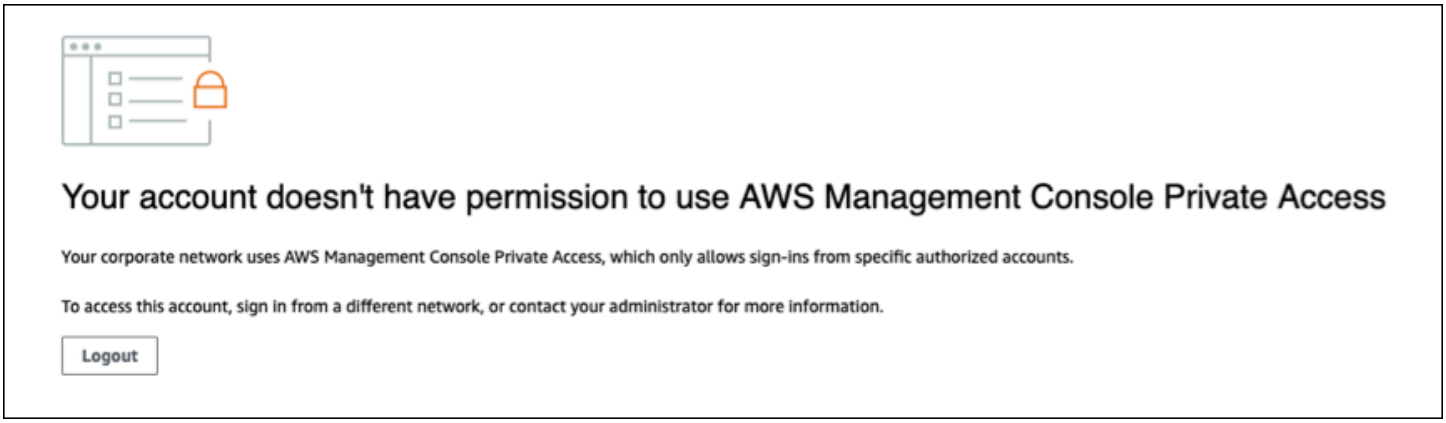
Die folgenden Richtlinien beschränken die Anmeldung auf ausgewählte Benutzer AWS-Konto IDs mithilfe einer AWS-Managementkonsole privaten Zugriffsrichtlinie für den Anmeldeendpunkt.

JSON

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

```
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "AWSAccountID"
                    ]
                }
            }
        }
    ]
}
```

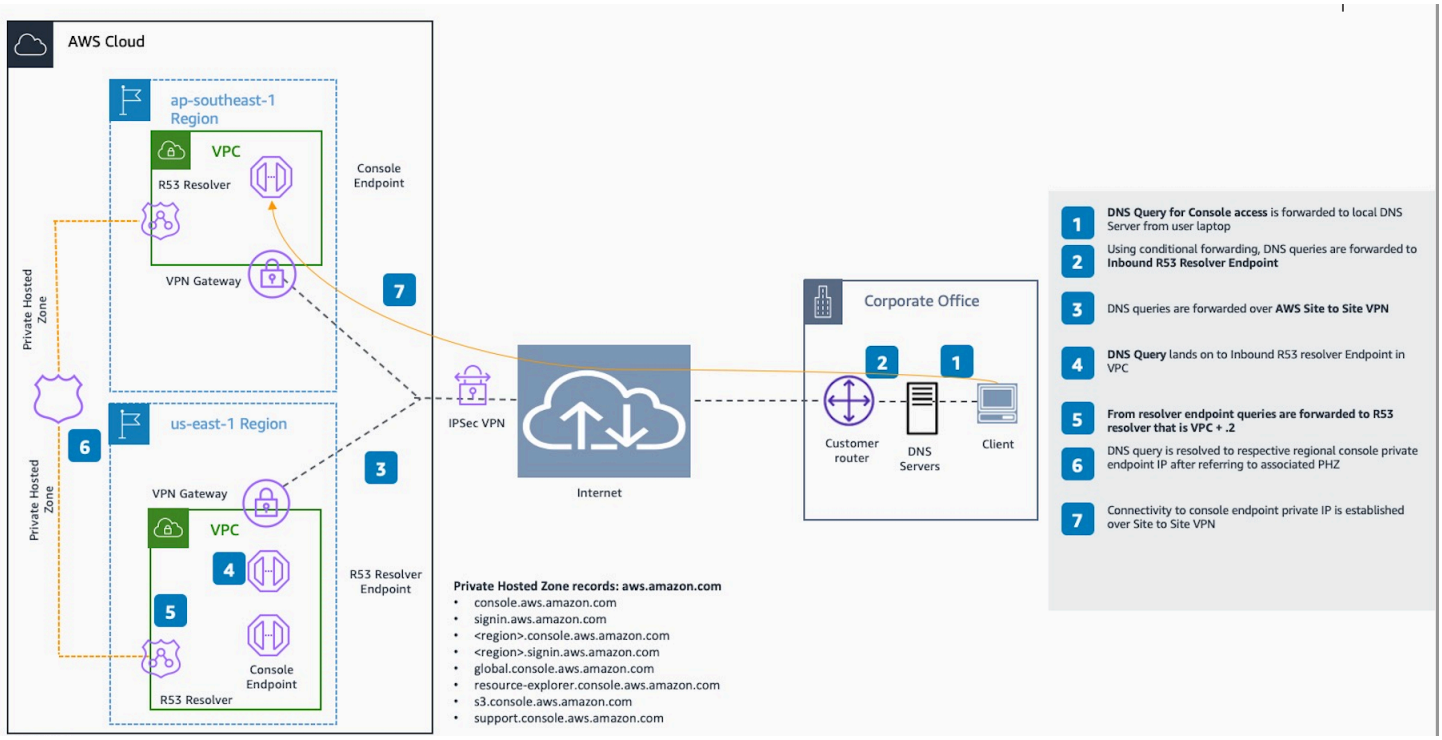
Wenn Sie eine Verbindung mit einer Identität herstellen, die nicht zu Ihrem Konto gehört, wird die folgende Fehlerseite angezeigt.



Referenzarchitektur

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

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



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

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

AWS Anpassung der Benutzererfahrung (UXC)

AWS Die Anpassung der Benutzererfahrung ermöglicht es Ihnen, Ihre AWS Benutzeroberflächen an Ihre spezifischen Bedürfnisse anzupassen und die Effizienz zu verbessern. UXC bietet derzeit eine Funktion zur Anpassung der Kontofarbe für Kontoadministratoren. Mit dieser Funktion können Administratoren je nach erforderlicher Gruppierung eine Farbe für ein Konto festlegen. Ein Administrator kann beispielsweise allen Produktionskonten Rot, allen Testkonten Gelb und allen Entwicklerkonten Grün zuweisen. Zu den Vorteilen der Anpassung der Kontofarbe gehören:

- Identifizieren Sie Kontotypen schnell visuell
- Geringeres Risiko von Änderungen an falschen Konten
- Gruppieren Sie ähnliche Konten (Produktion, Test, Entwicklung)

Zugriff auf die Anpassung der Benutzererfahrung

Sie können über Ihre Kontoseite im auf UXC zugreifen. AWS-Managementkonsole Weitere Informationen zum Zugriff auf diese Seite finden Sie unter???.

Erste Schritte mit der Anpassung AWS der Benutzererfahrung

Administratoren können Farben für verschiedene AWS Konten festlegen. Mithilfe der Kontofarben können Sie leicht zwischen den Konten unterscheiden, bei denen Sie derzeit angemeldet sind. Organizations können die Kontofarbe verwenden, um zwischen verschiedenen Kontotypen zu unterscheiden. Sie können beispielsweise Grün für Entwicklungskonten, Gelb für Testkonten und Rot für Produktionskonten verwenden.

> **Note**
>
> Für grundlegende Funktionen wie AWS User Experience Customization und Amazon Q sind entsprechende IAM-Berechtigungen erforderlich. AWS-Managementkonsole AWS CloudShell AWS verwaltete Richtlinien bieten eine bequeme Möglichkeit, diese Berechtigungen Benutzern und Rollen zu gewähren, die AWS-Managementkonsole innerhalb von verwendet werden. Die folgenden verwalteten Richtlinien können verwendet werden:
>
> - `AWSManagementConsoleBasicUserAccess`
>   - Für Benutzer ohne Administratorrechte

- Bietet Zugriff auf grundlegende Konsolenfunktionen
- `AWSManagementConsoleAdministratorAccess`
  - Für Benutzer mit Administratorrechten
  - Bietet Zugriff auf wichtige AWS-Managementkonsole Funktionen
  - Ermöglicht Administratoren die Konfiguration und Anpassung AWS-Managementkonsole für andere Identitäten

Weitere Informationen finden Sie unter ???.

Um eine Kontofarbe festzulegen

1. Melden Sie sich an der AWS-Managementkonsole an.
2. Wählen Sie auf der Navigationsleiste den Namen Ihres Kontos aus.
3. Wählen Sie Konto.
4. Wählen Sie in den Einstellungen für die Kontoanzeige eine Farbe aus.
5. Wählen Sie Aktualisieren aus.

API-Referenz

Die API-Referenz zur Anpassung der AWS Benutzererfahrung enthält Beschreibungen, API-Anforderungsparameter und die JSON-Antwort für jede der API-Aktionen zur Anpassung der AWS Benutzererfahrung.

Topics

- Aktionen
- Häufige Fehler

Aktionen

Folgende Aktionen werden unterstützt:

- ???
- ???

- ???

GetAccountColor

Ruft die dem Konto zugeordnete Farbe ab.

Anforderungssyntax

```
GET /v1/account-color HTTP/1.1
```

Die Anfrage verwendet keine URI-Parameter und enthält auch keinen Anforderungstext.

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
    "color": "string"
}
```

Antwortelemente

color

Die dem Konto zugeordnete Farbe.

Typ: Zeichenfolge

Gültige Werte: keine | pink | lila | dunkelblau | hellblau | blaugrün | grün | gelb | orange | rot

Fehler

Informationen zu Fehlern, die bei allen Aktionen auftreten, finden Sie unter Häufige Fehler.

AccessDeniedException

Der Benutzer verfügt nicht über ausreichende Zugriffsrechte, um diese Aktion auszuführen.

HTTP-Statuscode: 403

InternalServerException

Unerwarteter Fehler bei der Bearbeitung der Anfrage.

HTTP Status Code: 500

ThrottlingException

Die Anfrage wurde aufgrund einer Drosselung der Anfrage abgelehnt.

HTTP-Statuscode: 429

ValidationException

Diese Ausnahme wird ausgelöst, wenn das Benachrichtigungsereignis nicht validiert werden kann.

HTTP-Statuscode: 400

DeleteAccountColor

Löscht die Farbeinstellung für das Konto.

Anforderungssyntax

```
DELETE /v1/account-color HTTP/1.1
```

Anforderungsparameter

Dieser Vorgang verwendet keine Anforderungsparameter.

Anforderungstext

Dieser Vorgang besitzt keinen Anforderungstext.

Antworttext

Dieser Vorgang gibt keinen Antworttext zurück.

Fehler

Informationen zu Fehlern, die bei allen Aktionen auftreten, finden Sie unter Häufige Fehler.

AccessDeniedException

Der Benutzer verfügt nicht über ausreichende Zugriffsrechte, um diese Aktion auszuführen.

HTTP-Statuscode: 403

InternalServerException

Unerwarteter Fehler bei der Bearbeitung der Anfrage.

HTTP Status Code: 500

ThrottlingException

Die Anfrage wurde aufgrund einer Drosselung der Anfrage abgelehnt.

HTTP-Statuscode: 429

ValidationException

Diese Ausnahme wird ausgelöst, wenn das Benachrichtigungsereignis nicht validiert werden kann.

HTTP-Statuscode: 400

PutAccountColor

Legt die Farbe fest, die einem Konto zugeordnet ist.

Anforderungssyntax

```
PUT /v1/account-color HTTP/1.1
```

Anforderungstext

```
Content-type: application/json

{
   "color": "string"
}
```

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
    "color": "string"
```

```
}
```

Antwortelemente

color

Die Farbe, die dem Konto zugeordnet ist.

Typ: Zeichenfolge

Gültige Werte: keine | pink | lila | dunkelblau | hellblau | blaugrün | grün | gelb | orange | rot

Fehler

Informationen zu Fehlern, die bei allen Aktionen auftreten, finden Sie unter Häufige Fehler.

AccessDeniedException

Der Benutzer verfügt nicht über ausreichende Zugriffsrechte, um diese Aktion auszuführen.

HTTP-Statuscode: 403

InternalServerException

Unerwarteter Fehler bei der Bearbeitung der Anfrage.

HTTP Status Code: 500

ThrottlingException

Die Anfrage wurde aufgrund einer Drosselung der Anfrage abgelehnt.

HTTP-Statuscode: 429

ValidationException

Diese Ausnahme wird ausgelöst, wenn das Benachrichtigungsereignis nicht validiert werden kann.

HTTP-Statuscode: 400

Häufige Fehler

Die folgenden Fehler treten häufig bei API-Aktionen aller AWS Dienste auf. Informationen zu Fehlern, die für eine API-Aktion spezifisch sind, finden Sie in der Dokumentation zu dieser Aktion.

AccessDeniedException

Sie haben nicht genügend Zugriff, um diese Aktion auszuführen.

HTTP-Statuscode: 403

Weitere Informationen finden Sie unter Behebung von Fehlern bei Zugriffsverweigerung.

ExpiredTokenException

Das in der Anfrage enthaltene Sicherheitstoken ist abgelaufen.

HTTP-Statuscode: 403

IncompleteSignature

Die Signatur der Anfrage entspricht nicht den AWS Standards.

HTTP-Statuscode: 403

InternalFailure

Die Anforderungsverarbeitung ist fehlgeschlagen, da ein unbekannter Fehler, eine Ausnahme oder ein Fehler aufgetreten ist.

HTTP-Statuscode: 500

MalformedHttpRequestException

Es gibt Probleme mit der Anfrage auf HTTP-Ebene. Zum Beispiel können wir den Hauptteil nicht gemäß dem durch die Inhaltskodierung angegebenen Dekomprimierungsalgorithmus dekomprimieren.

HTTP-Statuscode: 400

NotAuthorized

Sie sind nicht berechtigt, diese Aktion auszuführen.

HTTP-Statuscode: 401

OptInRequired

Für die AWS Zugriffsschlüssel-ID ist ein Abonnement für den Dienst erforderlich.

HTTP-Statuscode: 403

RequestAbortedException

Die Anfrage wurde abgebrochen, bevor eine Antwort zurückgesendet wurde (z. B. hat der Client die Verbindung geschlossen).

HTTP-Statuscode: 400

RequestEntityTooLargeException

Es gibt Probleme mit der Anfrage auf HTTP-Ebene. Die Anforderungsentität ist zu groß.

HTTP-Statuscode: 413

RequestExpired

Die Anfrage erreichte den Service mehr als 15 Minuten nach dem Datumsstempel auf der Anfrage oder mehr als 15 Minuten nach dem Ablaufdatum der Anfrage (z. B. bei vorsignierter Anfrage URLs), oder der Datumsstempel auf der Anfrage liegt mehr als 15 Minuten in der future.

HTTP-Statuscode: 400

RequestTimeoutException

Es gibt Probleme mit der Anfrage auf HTTP-Ebene. Beim Lesen der Anfrage wurde das Timeout überschritten.

HTTP-Statuscode: 408

ServiceUnavailable

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP-Statuscode: 503

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

HTTP-Statuscode: 400

UnrecognizedClientException

Das angegebene X.509-Zertifikat oder die angegebene AWS Zugriffsschlüssel-ID ist in unseren Aufzeichnungen nicht vorhanden.

HTTP-Statuscode: 403

UnknownOperationException

Die angeforderte Aktion oder Operation ist ungültig. Überprüfen Sie, ob die Aktion ordnungsgemäß eingegeben wurde.

HTTP-Statuscode: 404

ValidationError

Die Eingabe erfüllt die von einem AWS Dienst angegebenen Einschränkungen nicht.

HTTP-Statuscode: 400

Protokollieren von API-Aufrufen zur Anpassung der AWS Benutzererfahrung mithilfe von AWS CloudTrail

AWS Die Anpassung der Benutzererfahrung ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem ausgeführten Aktionen bereitstellt AWS-Service. CloudTrail erfasst alle API-Aufrufe für UXC als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der UXC-Konsole und Codeaufrufen für die UXC-API-Operationen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an UXC gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, den Zeitpunkt der Anfrage und weitere Details ermitteln.

CloudTrail ist in Ihrem aktiv AWS-Konto , wenn Sie das Konto erstellen, und Sie haben automatisch Zugriff auf den CloudTrail Eventverlauf. Der CloudTrail Ereignisverlauf bietet eine einsehbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der aufgezeichneten Verwaltungsereignisse der letzten 90 Tage in einem. AWS-Region Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf. Für die Anzeige des Ereignisverlaufs CloudTrail fallen keine Gebühren an.

Für eine fortlaufende Aufzeichnung der Ereignisse in AWS-Konto den letzten 90 Tagen erstellen Sie einen Trail- oder CloudTrailLake-Event-Datenspeicher.

UXC-Managementereignisse in CloudTrail

Verwaltungsereignisse enthalten Informationen zu Verwaltungsvorgängen, die an Ressourcen in Ihrem AWS-Konto ausgeführt werden. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. CloudTrail Protokolliert standardmäßig Verwaltungsereignisse.

AWS Die Anpassung der Benutzererfahrung protokolliert alle Vorgänge auf der UXC-Steuerungsebene als Verwaltungsereignisse. Eine Liste der Vorgänge auf der Steuerungsebene zur Anpassung der AWS Benutzererfahrung, bei denen sich UXC anmeldet CloudTrail, finden Sie in der API-Referenz zur Anpassung der AWS Benutzererfahrung.

Beispiele für UXC-Ereignisse

Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über den angeforderten API-Vorgang, Datum und Uhrzeit des Vorgangs, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass Ereignisse nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt ein CloudTrail Ereignis, das den Vorgang demonstriert.


```
{
  "eventVersion" : "1.09",
  "userIdentity" : {
    "type" : "AssumedRole",
    "principalId" : "AIDACKCEVSQ6C2EXAMPLE:jdoe",
    "arn" : "arn:aws:sts::111122223333:assumed-role/user/jdoe",
    "accountId" : "111122223333",
    "accessKeyId" : "AKIAIOSFODNN7EXAMPLE",
    "sessionContext" : {
      "sessionIssuer" : {
        "type" : "Role",
        "principalId" : "AIDACKCEVSQ6C2EXAMPLE",
        "arn" : "arn:aws:iam::111122223333:role/user",
        "accountId" : "111122223333",
        "userName" : "jdoe"
      },
      "webIdFederationData" : { },
      "attributes" : {
        "creationDate" : "2022-12-09T23:48:51Z",
        "mfaAuthenticated" : "false"
      }
    }
  },
  "eventTime" : "2022-12-09T23:50:03Z",
  "eventSource" : "uxc.amazonaws.com",
  "eventName" : "GetAccountColor",
  "awsRegion" : "us-east-2",
  "sourceIPAddress" : "10.24.34.3",
```

```
  "userAgent" : "PostmanRuntime/7.43.4",
  "requestParameters" : null,
  "responseElements" : null,
  "requestID" : "543db7ab-b4b2-11e9-8925-d139e92a1fe8",
  "eventID" : "5b2805a5-3e06-4437-a7a2-b5fdb5cbb4e2",
  "readOnly" : true,
  "eventType" : "AwsApiCall",
  "managementEvent" : true,
  "recipientAccountId" : "111122223333",
  "eventCategory" : "Management"
}
```


Informationen zu CloudTrail Datensatzinhalten finden Sie im AWS CloudTrail Benutzerhandbuch unter CloudTrailDatensatzinhalt.

AWS verwaltete Richtlinien für die AWS-Managementkonsole

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSManagement ConsoleBasicUserAccess

Sie können `AWSManagementConsoleBasicUserAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Diese Richtlinie gewährt die erforderlichen Berechtigungen für Benutzer ohne Administratorrechte von. AWS-Managementkonsole Dazu gehören Funktionen wie Ressourcenerkennung, Benachrichtigungen, browserbasierter Shell-Zugriff und benutzerdefinierte Navigation.

Details zu Berechtigungen

Dies `AWSManagementConsoleBasicUserAccess` ist in die folgenden Gruppen von Berechtigungen unterteilt:

- `cloudshell`— Ermöglicht Prinzipalen vollen Zugriff auf AWS CloudShell Funktionen, einschließlich Umgebungserstellung, Sitzungsverwaltung und Befehlsausführung.
- `ec2`— Ermöglicht Prinzipalen die Beschreibung von Regionen, die für das Konto in Unified Navigation aktiviert sind.
- `notifications`— Ermöglicht Prinzipalen das Abrufen von Ereignissen von. AWS-Benutzerbenachrichtigungen
- `q`— Ermöglicht Principals, mit Amazon Q Developer zu chatten.
- `resource-explorer-2`— Ermöglicht Prinzipalen das Suchen und Entdecken von AWS Ressourcen mithilfe von Unified Search.
- `uxc`— Ermöglicht Prinzipalen das Lesen der Einstellungen zur Anpassung AWS der Benutzererfahrung.
- `action-recommendations`— Ermöglicht es den Prinzipalen, kontextbezogene Handlungsempfehlungen zu erhalten.
- `account`— Ermöglicht Prinzipalen das Abrufen von Informationen über das angegebene Konto, einschließlich des Kontonamens, der Konto-ID sowie des Datums und der Uhrzeit der Kontoerstellung.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSManagementConsoleBasicUserAccess in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSManagement ConsoleAdministratorAccess

Sie können `AWSManagementConsoleAdministratorAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Diese Richtlinie gewährt vollen Zugriff zur Konfiguration und Anpassung von AWS-Managementkonsole. Sie ermöglicht es Administratoren, Kontofarben festzulegen, Benutzerbenachrichtigungen zu aktivieren und die Ressourcenerkennung zu konfigurieren. Dazu gehören auch Berechtigungen aus der `AWSManagementConsoleBasicUserAccess` verwalteten Richtlinie, die für Benutzer ohne Administratorrechte unerlässlich sind. AWS-Managementkonsole

Details zu Berechtigungen

Dies `AWSManagementConsoleAdministratorAccess` ist in die folgenden Gruppen von Berechtigungen unterteilt:

- `cloudshell`— Ermöglicht Prinzipalen vollen Zugriff auf AWS CloudShell Funktionen, einschließlich Umgebungserstellung, Sitzungsverwaltung und Befehlsausführung.
- `ec2`— Ermöglicht Prinzipalen die Beschreibung von Regionen, die für das Konto in Unified Navigation aktiviert sind.
- `notifications`— Ermöglicht Prinzipalen den Zugriff auf Benachrichtigungskonfigurationen, Ereignisse und den Opt-In-Status von Funktionen und deren Aktualisierung.
- `q`— Ermöglicht Principals, mit Amazon Q Developer zu chatten, um KI-gestützten Support zu erhalten.
- `resource-explorer-2`— Ermöglicht Prinzipalen das Suchen und Entdecken von AWS Ressourcen mithilfe von Unified Search.
- `uxc`— Ermöglicht Prinzipalen vollen Zugriff auf die Einstellungen zur Anpassung AWS der Benutzererfahrung.
- `action-recommendations`— Ermöglicht es den Prinzipalen, kontextbezogene Handlungsempfehlungen zu erhalten.
- `account`— Ermöglicht Prinzipalen das Abrufen von Informationen über das angegebene Konto, einschließlich des Kontonamens, der Konto-ID sowie des Datums und der Uhrzeit der Kontoerstellung.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSManagementConsoleAdministratorAccess in der Referenz zu von AWS verwalteten Richtlinien.

AWS-Managementkonsole Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen der AWS verwalteten Richtlinien AWS-Managementkonsole seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst. Abonnieren Sie den RSS-Feed auf der Seite AWS-Managementkonsole Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderungen	Beschreibung	Date
AWSManagementConsoleBasicUserAccess – Richtlinie aktualisieren	Die Richtlinie wurde aktualisiert, sodass nun Berechtigungen hinzugefügt wurden, mit denen Benutzer beim Navigieren auf der Seite Kontoinformationen einsehen und Handlungsempfehlungen erhalten können. AWS-Managementkonsole	9. Dezember 2025
AWSManagementConsoleAdministratorAccess – Richtlinie aktualisieren	Die Richtlinie wurde aktualisiert, sodass Benutzer beim Navigieren im Bereich Kontoinformationen einsehen und Handlungsempfehlungen erhalten können. AWS-Managementkonsole	9. Dezember 2025
AWSManagementConsoleBasicUserAccess – Neue Richtlinie	Es wurde eine neue AWS verwaltete Richtlinie hinzugefügt, die Berechtigungen gewährt, die für die grundlegende AWS-Managementkonsole Navigation, die Anzeige von Kontofarben und die	14. August 2025

Änderungen	Beschreibung	Date
	Ressourcensuche erforderlich sind.	
AWSManagementConsoleAdministratorAccess – Neue Richtlinie	Es wurde eine neue AWS verwaltete Richtlinie hinzugefügt, die vollen Zugriff auf die Konfiguration und Anpassung von bietet AWS-Managementkonsole.	14. August 2025
AWS-Managementkonsole hat begonnen, Änderungen zu verfolgen	AWS-Managementkonsole hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	14. August 2025

Verwenden von Markdown in der Konsole

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

Inhalt

Paragraphen, Zeilenabstand und horizontale Linien

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

```
 

 
```

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

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

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

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

Überschriften

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

```
# Top-level heading
```

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

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

Textformatierung

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

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

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

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

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

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

Links

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

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

Listen

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

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

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

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

Tabellen und Schaltflächen (CloudWatch Dashboards)

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

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

```
Table | Header
```

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

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

Tabelle	Kopfzeile
Amazon Web Services	AWS
1	2

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

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

Fehlerbehebung

In diesem Abschnitt finden Sie Lösungen für häufig auftretende Probleme mit dem AWS-Managementkonsole.

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

Themen

Die Seite wird nicht ordnungsgemäß geladen.

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

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

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

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

Kürzlich an der Konsole vorgenommene Änderungen können sich auf Ihren Zugriff auswirken, wenn alle der folgenden Bedingungen erfüllt sind:

- Sie greifen AWS-Managementkonsole von einem Netzwerk aus zu, das so konfiguriert ist, dass es AWS Dienstendpunkte über VPC-Endpunkte erreicht.
- Sie schränken den Zugriff auf AWS Dienste ein, indem Sie entweder den `aws:SourceVpc` globalen Bedingungsschlüssel in Ihren IAM-Richtlinien verwenden`aws:SourceIp`.

Wir empfehlen Ihnen, die IAM-Richtlinien zu überprüfen, die den `aws:SourceIp` oder den `aws:SourceVpc` globalen Bedingungsschlüssel enthalten. Wenden Sie beide `aws:SourceVpc` an `aws:SourceIp` und wo zutreffend.

Einige AWS-Managementkonsole Funktionen verwenden Dual-Stack-Domänen, die IPv4 sowohl IPv6 Verbindungen als auch unterstützen. Wenn Ihre IAM-Richtlinie den Zugriff nur `aws:SourceIp` mithilfe von IPv4 CIDR-Blöcken einschränkt, schlagen Anfragen möglicherweise fehl, wenn Ihr

Betriebssystem IPv6 Verbindungen bevorzugt (oder umgekehrt). Um dies zu vermeiden, sollten Sie sowohl als auch IPv4 IPv6 CIDR-Blöcke in Ihre Bedingung aufnehmen. `aws:SourceIp` Weitere Informationen finden Sie unter aws: SourceIp im AWS Identity and Access Management Benutzerhandbuch.

Sie können auch die AWS-Managementkonsole Private Access-Funktion nutzen, um AWS-Managementkonsole über einen VPC-Endpunkt darauf zuzugreifen und die `aws:SourceVpc` Bedingungen in Ihren Richtlinien zu verwenden. Weitere Informationen finden Sie hier:

- AWS-Managementkonsole Privater Zugang
- the section called “So funktioniert AWS-Managementkonsole Private Access mit aws: SourceVpc”
- the section called “Unterstützte Kontextschlüssel für AWS globale Bedingungen”

Mein Browser zeigt Timeout-Fehler an, wenn ich eine Verbindung zum AWS-Managementkonsole

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

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

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

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

Ich möchte die Sprache von ändern, finde AWS-Managementkonsole aber das Sprachauswahlmenü unten auf der Seite nicht

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

Weitere Informationen finden Sie unter Ändern der Sprache der AWS-Managementkonsole.

Dokumentverlauf

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

Änderungen	Beschreibung	Datum
Seite hinzugefügt	Neue Seite zur Erläuterung der empfohlenen Maßnahmen hinzugefügt. Weitere Informationen finden Sie unter ???.	15. Oktober 2025
Neue AWS verwaltete Richtlinien	Dem Geltungsbereich der Berechtigungen für die Verwendung, Konfiguration und Anpassung von wurden zwei neue Richtlinien hinzugefügt. AWS-Managementkonsole • AWSManagementConsoleBasicUserAccess • AWSManagementConsoleAdministratorAccess	14. August 2025
Anpassungen der Benutzererfahrung (UXC)	Neuer Service verfügbar.	14. August 2025
Seite aktualisiert	Sie können Ihre Anwendungen jetzt über das Menü Dienste in MyApplications einsehen. Weitere Informationen finden Sie unter ???.	29. Juli 2025
Seite hinzugefügt	Neue Seite hinzugefügt, um die Multisession-Funktion zu	6. Dezember 2024

Änderungen	Beschreibung	Datum
	erklären. Weitere Informati onen finden Sie unter ???.	
Seite aktualisiert	Die Seite zum Ändern Ihres Passworts wurde aktualisiert. Weitere Informationen finden Sie unter ???.	18. Juni 2024
Neue Seiten hinzugefügt	Es wurden neue Seiten hinzugefügt, auf denen beschrieben wird, wie Sie auf das Menü Dienste und auf AWS Ereignisbenachrich tigungen zugreifen können. Weitere Informationen erhalten Sie unter ??? und ???.	18. Juni 2024
Seite aktualisiert	Was ist der AWS-Manag ementkonsole? Seite aktualisi ert. Weitere Informationen finden Sie unter ???.	18. Juni 2024
Holen Sie sich Unterstützung	Es wurde eine neue Seite hinzugefügt, auf der beschrieb en wird, wie Sie Support erhalten können. Weitere Informationen finden Sie unter ???.	18. Juni 2024
Vereinheitlichte Navigation und AWS Console Home	Es wurden neue Seiten hinzugefügt, auf denen beschrieben wird, wie man mit der Konsole arbeitet. Weitere Informationen erhalten Sie unter ??? und ???.	18. Juni 2024

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

Änderungen	Beschreibung	Datum
Ändern der Konsolensprache	Auswahl einer anderen Sprache für die AWS-Management konsole. Weitere Informationen finden Sie unter Ändern der Sprache der AWS-Managementkonsole.	1. April 2021
Wird gestartet CloudShell	Öffnen Sie AWS CloudShell über die AWS CLI-Befehle AWS-Managementkonsole und führen Sie sie aus. Weitere Informationen finden Sie unter Starten AWS CloudShell.	22. März 2021

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.